NIST Special Publication 500-210

Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

APPLICATION PORTABILITY PROFILE (APP) The U.S. Government's Open System Environment Profile OSE/1 Version 2.0

APPLICATION PORTABILITY PROFILE
APP The U.S. Government's Open System Environment Profile OSE/1 Version 2.0

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering and performs related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Robot Systems
- Factory Automation
- Fabrication Technology

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services[2]
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 500-210

APPLICATION PORTABILITY PROFILE (APP) The U.S. Government's Open System Environment Profile OSE/1 Version 2.0

Systems and Software Technology Division
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

Supersedes NIST Special Publication 500-187

June 1993

U.S. DEPARTMENT OF
Ronald H. Brown, Secret
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-210
Natl. Inst. Stand. Technol. Spec. Publ. 500-210, 103 pages (June 1993)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1993

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Executive Summary

Federal information systems initially developed from isolated islands of computing. Through progressive changes, these individual systems became connected by common users and common information needs. These systems are now well on the way to migrating toward computing environments that consist of distributed, heterogeneous, networked applications, databases, and hardware. The concept of a Federal computing environment that is built on an infrastructure defined by open, consensus-based standards is well on its way to becoming a de facto means of organizing these systems. Such an infrastructure is called an Open System Environment (OSE).

An Open System Environment encompasses the functionality needed to provide interoperability, portability, and scalability of computerized applications across networks of heterogeneous, multi-vendor hardware/software/communications platforms. The OSE forms an extensible framework that allows services, interfaces, protocols, and supporting data formats to be defined in terms of nonproprietary specifications that evolve through open (public), consensus-based forums.

A selected suite of specifications that defines the interfaces, services, protocols, and data formats for a particular class or domain of applications is called a profile. The Application Portability Profile (APP) integrates industry, Federal, national, international, and other specifications into a Federal application profile to provide the functionality necessary to accommodate a broad range of Federal information technology requirements.

This report, a.k.a the APP Guide, is designed to provide recommendations on a variety of specifications that will generally fit the requirements of U.S. Government systems. A specific organization will not necessarily require all of the recommended specifications in the APP. As the U.S. Government's OSE profile, this guidance is provided to assist Federal agencies in making informed choices regarding the selection and use of OSE specifications, and in the development of more selective application profiles based on the APP. It is directed toward managers and project leaders who have the responsibilities of acquiring, developing, and maintaining information systems supported by heterogeneous application platform environments.

The APP is <u>not</u> a standard and is not designed to cover every case. In some instances, the selection of one specification recommended in the APP will obviate the need for other specifications that are also recommended (i.e., select one or the other, but not both.) There is some overlap in functionality covered in different specifications. There are also gaps in functionality. In areas where the APP does not meet all of a user's requirements, the user must augment the recommended specifications to ensure that proposed systems built on these specifications meet organizational requirements. This report is designed to help users determine which specifications to use.

Many specifications were reviewed and evaluated before the final recommended specifications were selected. If there are other specifications that should be considered in the APP and that meet a broad range of U.S. government application requirements, users, vendors, and other interested parties should formally recommend them for evaluation

using the same evaluation criteria applied to the selected specifications. This is one of the ways in which the APP will continue to evolve as technology evolves.

The initial version of the APP was published by the National Institute of Standards and Technology (NIST) in April 1991 as Special Publication 500-187. The changes in this revision reflect the evolutionary process developments that have occurred in the standards arena. Specifically, Version 2 of the APP Guide incorporates the following:

a) updated information on each recommended specification;
b) the addition of many new specifications with the results of evaluation;
c) editorial changes, and additions where applicable; and
d) several new sections to provide guidance where agencies have requested information and posed questions.

The mention of specification names in certain instances should not be interpreted to mean that the National Institute of Standards and Technology (NIST) endorses the acquisition of any specific products based on these specifications. NIST has endeavored to separate references to the specifications from products and services, and has provided evaluation criteria, where applicable, to enable users to make their own judgements of the applicability of the recommended specifications to their requirements. For specific individual and organizational requirements, other specifications not mentioned here may be more applicable.

A warning must be given to users of this report. Wholesale inclusion of this report, the APP Guide, by reference in procurement documents through statements such as "Products shall conform to the APP Guide," or similar wording is a misuse of this information. Such actions will not guarantee that the acquiring organization has adequately addressed organizational and technical requirements. As a matter of fact, such actions will probably ensure that an organization will travel in a direction other than the intended one. Some specifications overlap others, and the selection of one specification may conflict with or prevent the use of another.

The intended use of this report is as a catalog from which thoughtful selections can be made in response to clearly defined user requirements. Individual recommendations and specifications in this report must be reviewed by the acquiring agencies to determine if they are applicable to a specific acquisition and whether or not the specifications are adequate to describe the organization's requirements. In addition, inasmuch as there is overlap among some of the specifications recommended, the acquiring agencies must ensure that requirements do not conflict with one another, nor with internal organizational policy.

Contents

Figures

Tables

1. INTRODUCTION

Federal agencies are under increasing pressure to use information technology to improve efficiency and delivery of services to the public. At the same time, there is a new reality that is becoming increasingly evident. Key aspects of this new reality are that Federal agencies—

a) now recognize that they can no longer create de jure standards and enforce them on the commercial market as they were able to do with early standards;

b) must rely on the commercial market for information technology products and services; and

c) must establish strategies and plans for acquiring information technology products and services based upon open system standards that support application software portability, scalability, and interoperability.

Systems within Federal agencies typically are developed in an environment of isolated islands of computing. Now there is interdependence of users and systems across the entire organization. This interdependence has served to highlight enterprise-wide needs for common application architectures, communication networks, and databases. This interdependence has also raised concerns about computer security issues and the need to address those issues from policy, management, and technical perspectives.

One of the most significant factors underlying the changing technology is that Federal and nonfederal users now recognize that no single vendor can supply all of their needs for information technology systems and services. Since very large homogeneous environments are no longer practical in many cases, users need open systems that provide interoperability of products and portability of people, data, and applications throughout heterogenous computing environments.

The need to improve portability and interoperability has resulted in widespread interest in standards such as the Portable Operating System Interface for Computing Environments (POSIX) and Government Open System Interconnection Profile (GOSIP). Whereas development of these standards are important milestones in the effort to achieve portability and interoperability, POSIX and GOSIP are not sufficient to address the full spectrum of needs, even within their stated scopes of concern.

1.1 Scope

The focus of this guide is on open system environments (OSE) which integrate POSIX, GOSIP, and other specifications to provide the functionality necessary to address a broad range of Federal information technology requirements. The guidance is intended to assist Federal agencies in making informed choices regarding the selection and use of OSE specifications, and in the development of OSE profiles. This guidance is directed toward managers and project leaders who have the responsibilities of acquiring, developing, and

maintaining information systems supported by heterogeneous hardware/software/communications platforms. Since the specifications described are highly technical in nature, users of this guidance should consult with subject area experts to determine the applicability of each specification to a particular organizational objective.

Ideally, specifications would be expressed in terms of international standards. Unfortunately, there are areas of OSE functionality for which formal standards, much less international standards, do not exist. Although this situation will improve over time, users who have requirements for those functions are faced with the question, "What specifications should I use now?"

1.2 Purpose

The Application Portability Profile (APP) is directed toward assisting managers, project leaders, and users in making an informed judgment regarding the choice of specifications to meet current requirements. There are two dimensions of the assistance provided. First, specifications are provided for each functional service area described in the APP. The specifications represent the collective judgment of the National Institute of Standards and Technology (NIST) Computer System Laboratory's (CSL) staff regarding the most appropriate specification for each functional area. Second, and equally as important, evaluation criteria to assist in making qualitative assessments of the recommended specifications are defined and applied. Application of these evaluation criteria resulted in the NIST assessments of the suitability of the specifications recommended.

Users of the APP should use the evaluation criteria to make their own assessments of the recommended specifications. Further, users should consider assigning weighted values to elements of the criteria based on their judgments of the relative importance to be given to each element. Users should also consider requiring vendors to use the evaluation criteria to assess specifications that the vendors choose to propose as an alternative to the specifications recommended in this document.

The following sections briefly describe the meaning of open system environment, the OSE Reference Model, and specific components of the Application Portability Profile. Later sections provide recommended specifications for specific APP components. References for further information and addresses of organizations that distribute documents on the recommended specifications are included toward the end of this report.

2. ACRONYMS

2.1 **AAP:** Association of American Publishers
2.2 **ACSE:** Association Control Service Element
2.3 **AJPO:** Ada Join Program Office
2.4 **ANS:** American National Standard
2.5 **ANSI:** American National Standards Institute
2.6 **AOW:** Asiatic Oceania Workshop
2.7 **API:** Application Program Interface
2.8 **APP:** Application Portability Profile
2.9 **APTL:** Accredited POSIX Testing Laboratory
2.10 **ASI:** Application Software Interface
2.11 **ASME:** American Society of Mechanical Engineers
2.12 **ASN.1:** Abstract Syntax Notation One
2.13 **BRI:** Basic Rate Interface
2.14 **BSD:** Berkeley Systems Development
2.15 **CAD/CAM:** Computer-Aided Design and Manufacturing
2.16 **CADETC:** CAD/CAM Data Exchange Technical Centre
2.17 **CAE:** Computer Application Environment
2.18 **CALS:** Computer-Aided Acquisition and Logistic Support
2.19 **CASE:** Computer-Aided Software Engineering (See ISEE)
2.20 **CCITT:** International Telegraph and Telephone Consultative Committee
2.21 **CGM:** Computer Graphics Metafile
2.22 **CMP:** Completeness
2.23 **CMW:** Compartmented Mode Workstation
2.24 **COS:** Corporation for Open Systems
2.25 **COSMIC:** Computer Software Management and Information Center
2.26 **CSL:** Computer Systems Laboratory (part of NIST)
2.27 **DAC:** Discretionary Access Control
2.28 **DBMS:** Database Management System
2.29 **DCE:** Distributed Computing Environment
2.30 **DFU:** De Facto Usage
2.31 **DIA:** Defense Intelligence Agency
2.32 **DIS:** Draft International Standard
2.33 **DNI:** Detailed Network Interface
2.34 **DPANS:** Draft Proposed American National Standard
2.35 **DoD:** Department of Defense
2.36 **DTD:** Document Type Definition
2.37 **ECMA:** European Computer Manufacturers Association
2.38 **ECMA/TC33:** European Computer Manufacturers Association Technical Committee 33
2.39 **ECMA PCTE:** European Computer Manufacturers Association Portable Common Tools Environment
2.40 **EDI:** Electronic Data Interchange
2.41 **EDIFACT:** Electronic Data Interchange For Administration, Commerce, and Transport

2.42 **EEI:** External Environment Interface
2.43 **EMPM:** Electronic Manuscript Preparation and Markup
2.44 **EPRI:** Electric Power Research Institute
2.45 **EWOS:** European Workshop on Open Systems
2.46 **FDDI:** Fiber Distributed Data Interface
2.47 **FIPS:** Federal Information Processing Standard
2.48 **FIPS PUB:** Federal Information Processing Standard Publication
2.49 **FTAM:** File Transfer, Access and Management
2.50 **GCA:** Graphics Communication Association
2.51 **GIS:** Geographic Information System
2.52 **GKS:** Graphical Kernel System
2.53 **GORD:** GOSIP Register Database
2.54 **GOSIP:** Government Open System Interconnection Profile
2.55 **GUI:** Graphical User Interface
2.56 **HCI:** Human/Computer Interface
2.57 **ICCCM:** Inter-Client Communications Conventions Manual
2.58 **IDRP:** Inter-Domain Routing Protocol
2.59 **IEC:** International Electrotechnical Commission
2.60 **IEEE:** Institute of Electrical and Electronics Engineers
2.61 **IGES:** Initial Graphics Exchange Specification
2.62 **IGOSS:** Industry/Government Open Systems Specification
2.63 **INTAP:** Interoperability Technology Association for Information Processing
2.64 **IRDS:** Information Resource Dictionary System
2.65 **IS-IS:** Intermediate System-Intermediate System
2.66 **ISDN:** Integrated Services Digital Network
2.67 **ISEE:** Integrated Software Engineering Environment
2.68 **ISO:** International Organization for Standardization
2.69 **ISO/IEC:** International Organization for Standardization/International Electrotechnical Commission
2.70 **JITC:** Joint Interoperability Test Center
2.71 **JTC1:** Joint Technical Committee One
2.72 **LAN:** Local Area Network
2.73 **LAPD:** Link Access Procedures D
2.74 **LIS:** Language Independent Specification
2.75 **LOC:** Level of Consensus
2.76 **MAC:** Mandatory Access Control
2.77 **MAN:** Metropolitan Area Network
2.78 **MAP/TOP:** Manufacturing Automation Protocol/Technical and Office Protocols
2.79 **MAT:** Maturity
2.80 **MHS:** Message Handling Service
2.81 **NASA:** National Aeronautics and Space Administration
2.82 **NBSIR:** National Bureau of Standards Interim Report
2.83 **NCC:** National Computing Centre
2.84 **NCGA:** National Computer Graphics Association
2.85 **NCSC:** National Computer Security Center
2.86 **NI-X:** Bellcore National ISDN-X
2.87 **NISO:** National Information Standards Organization

2.88 **NIST:** National Institute of Standards and Technology
2.89 **NIU-Forum:** North American ISDN Users' Forum
2.90 **NIUF:** North American ISDN Users' Forum
2.91 **NTIS:** National Technical Information Service
2.92 **NVLAP:** National Voluntary Laboratory Accreditation Program (NIST-sponsored program)
2.93 **ODA/ODIF/ODL:** Open Document Architecture/Open Document Interchange Format/Open Document Language
2.94 **OIW:** OSE Implementor's Workshop
2.95 **OMG:** Object Management Group
2.96 **OSE:** Open System Environment
2.97 **OSE/RM:** Open System Environment Reference Model
2.98 **OSF:** Open Software Foundation
2.99 **OSI:** Open System Interconnection
2.100 **PAV:** Product Availability
2.101 **PDES:** Product Data Exchange using STEP
2.102 **PHIGS:** Programmer's Hierarchical Interactive Graphics System
2.103 **PII:** Protocol Independent Interfaces
2.104 **POSIX:** Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]
2.105 **PRI:** Primary Rate Interface
2.106 **PRL:** Problems/Limitations
2.107 **RDA:** Remote Database Access
2.108 **RPC:** Remote Procedure Call
2.109 **SDIF:** Standard Document Interchange Format
2.110 **SDTS:** Spatial Data Transfer Specification
2.111 **SGML:** Standard Generalized Markup Language
2.112 **SNI:** Simple Network Interface
2.113 **SPDL:** Standard Page Description Language
2.114 **SQL:** Structured Query Language
2.115 **STB:** Stability
2.116 **STEP:** Standard for the Exchange of Product Model Data
2.117 **SVID:** System V Interface Definition
2.118 **TEI:** Text Encoding Initiative
2.119 **TFA:** Transparent File Access
2.120 **UAC:** User Advisory Council
2.121 **UI:** UNIX International
2.122 **UN/ECE/WP.4:** United Nations Economic Commission for Europe, Working Party Four on Trade Facilitation
2.123 **USGS:** U.S. Geological Survey
2.124 **VAN:** Value-Added Network
2.125 **VPL:** Validated Products List
2.126 **WAN:** Wide Area Network
2.127 **WYSIWYG:** What You See Is What You Get

2.128 **X3:** Technical Committee X3 - Information Processing Systems
2.129 **XPG4:** X/Open Portability Guide Issue 4
2.130 **XTI:** X/Open Transport Interface

3. OPEN SYSTEM ENVIRONMENT

From the perspective of users and technologists alike, an open system environment (OSE) consists of a computing support infrastructure which facilitates the acquisition of applications that—

a) execute on any vendor's platform;
b) use any vendor's operating system;
c) access any vendor's database;
d) communicate and interoperate over any vendor's networks;
e) are secure and manageable; and
f) interact with users through a common human/computer interface.

In more technical terms, an OSE is a computing environment that supports portable, scalable, and interoperable applications through standard services, interfaces, data formats, and protocols. The standards may consist of international, national, industry, or other open (public) specifications. These specifications are available to any user or vendor for use in building systems and products that meet OSE criteria.

Applications in an OSE are scalable among a variety of platform and network configurations, from standalone microcomputers, to large distributed systems that may include microcomputers, workstations, minicomputers, mainframes, and supercomputers, or any configuration in between. The existence of greater or fewer computing resources on any platform will be apparent to users only in the context that they affect the application's speed of execution, for example in how fast screens are refreshed or data is retrieved, or the capacity of each platform to process data (i.e., 16-bit data bus versus a 32-bit bus).

Applications interoperate by using standard communication protocols, data interchange formats, and distributed system interfaces to transmit, receive, understand, and use information. The process of moving information from one platform, through a local area network, wide area network, or combination of networks to other platforms should be transparent to the application and the user. Locations of other platforms, users, databases, and programs should also be transparent to the application.

In short, an OSE supports applications through the use of well-defined components: a plug-compatible technology or building-block approach for developing systems.

Unfortunately, not enough standards are in place to define an OSE completely. Standards organizations are working on this problem, but much effort is still needed. As technology changes, some standards will become obsolete and other new ones will be required. Organizations can still accomplish a great deal in moving toward an OSE by selecting specifications that will provide greater openness over time.

3.1 OSE Reference Model

The Institute of Electrical and Electronics Engineers (IEEE) POSIX Working Group P1003.0 describes an OSE Reference Model (OSE/RM) that is closely aligned with the APP and that provides a framework for describing open system concepts and defining a lexicon of terms that can be agreed upon generally by all interested parties. Figure 1 illustrates the OSE/RM.

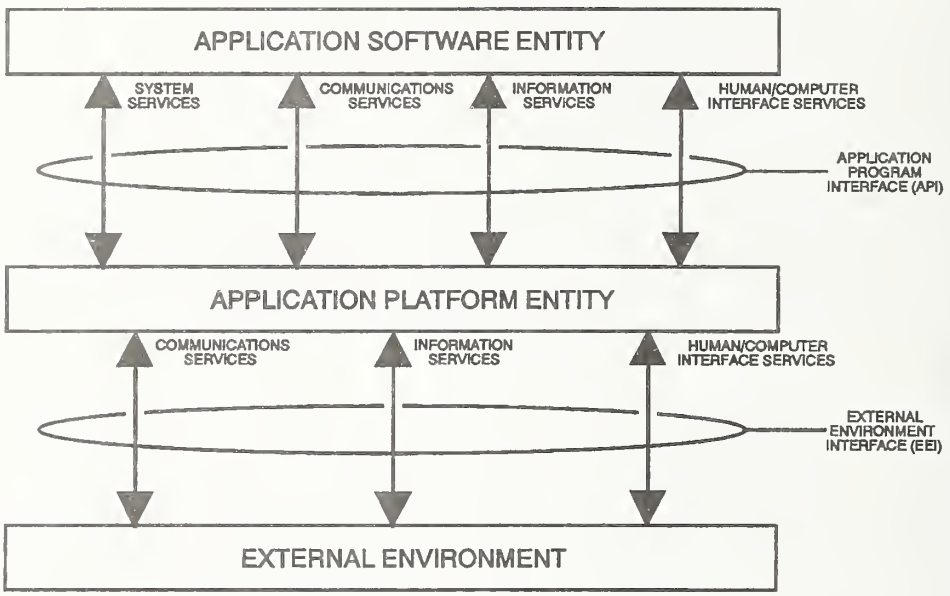

Figure 1. Open System Environment Reference Model (OSE/RM).

Two types of elements are used in the model: entities consisting of the application software, application platform, and platform external environment; and interfaces including the application program interface and external environment interface.

The three classes of OSE reference model entities are described as follows:

a) **Application Software** — Within the context of the OSE Reference Model, the application software includes data, documentation, and training, as well as programs.

b) **Application Platform** — The application platform is composed of the collection of hardware and software components that provide the system services used by application software.

c) **Platform External Environment** — The platform external environment consists of those system elements that are external to the application software and the application platform (e.g., services provided by other platforms or peripheral devices).

There are two classes of interfaces in the OSE reference model, as described in the following paragraphs:

a) **Application Program Interface (API)** — The API is the interface between the application software and the application platform. Its primary function is to support portability of application software. An API is categorized in accordance with the types of service accessible via that API. There are four types of API services in the OSE/RM:

   1) Human/computer interface services
   2) Information interchange services
   3) Communication services
   4) Internal system services

b) **External Environment Interface (EEI)** — The EEI is the interface that supports information transfer between the application platform and the external environment, and between applications executing on the same platform. Consisting chiefly of protocols and supporting data formats, the EEI supports interoperability to a large extent. An EEI is categorized in accordance with the type of information transfer services provided. There are three types of information transfer services. These are transfer services to and from:

   1) Human users
   2) External data stores
   3) Other application platforms

In its simplest form, the OSE/RM illustrates a straightforward user-supplier relationship: the application software is the user of services and the application platform/external environment entities are the suppliers. The API and EEI define the services that are provided.

3.2 OSE Profile and the APP

A profile consists of a selected list of standards and other specifications that define a complement of services made available to applications in a specific domain. Examples of domains might include a workstation environment, an embedded process control environment, a distributed environment, a transaction processing environment, or an office automation environment, to name a few. Each of these environments has a different cross-section of service requirements that can be specified independently from the others. Each service, however, is defined in a standard form across all environments.

An OSE profile is composed of a selected list of open (public), consensus-based standards and specifications that define services in the OSE/RM. Restricting a profile to a specific domain or group of domains that are of interest to an individual organization results in the definition of an organizational profile. The Application Portability Profile (APP) is an OSE profile designed for use by the U.S. Government. It covers a broad range of application software domains of interest to many Federal agencies, but it does not include

every domain within the U.S. Government's application inventory. The individual standards and specifications in the APP define data formats, interfaces, protocols, or a mix of these elements.

3.3 APP Service Areas

The services defined in the APP tend to fall into seven broad service areas. These service areas are:

a) operating system services
b) human/computer interface services
c) data management services
d) data interchange services
e) software engineering services
f) graphics services
g) network services

Each service area is defined in the following sections. Figure 2 illustrates where each of these seven services areas relates to the OSE/RM. (Assume that software engineering services are applicable in all areas.)

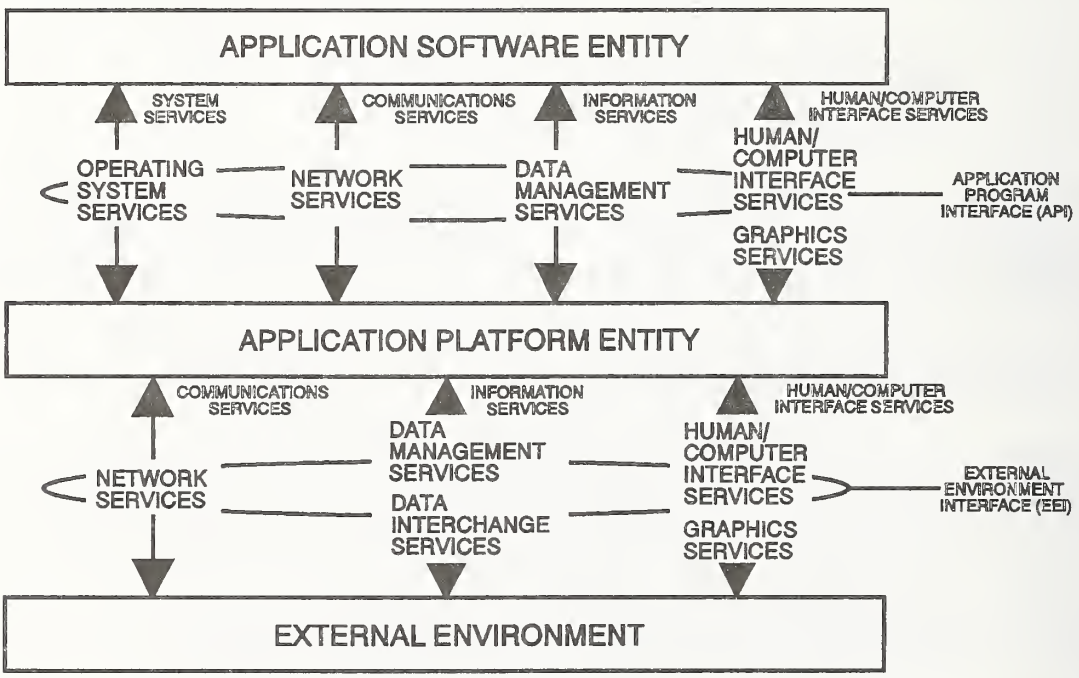

Figure 2. APP Service Areas and the OSE/RM.

Each of the APP **service areas** addresses specific components around which interface, data format, or protocol specifications have been or will be defined. Security and management services are common to all of the service areas and pervade these areas in one or more forms.

Currently, specifications for security can be recommended in operating system services, network services, and access control and integrity constraints for data management services. Specifications for security in the other service areas are not sufficiently advanced to warrant inclusion at this time.

Management services are partly defined and still under development. They are based on the Open System Interconnection (OSI) Network Management Framework, which applies mainly to the overlap among network, system, and application management functions (see fig. 3). This overlapping area applies equally to networks and individual nodes on networks and forms the framework for the OSI approach to systems and network management. Other management functions in the typical operating system sense (e.g., user accounts, resource administration, etc.) will be added over time. As these specifications mature and stabilize, they will be reviewed and appropriate ones may be selected for use in the APP.

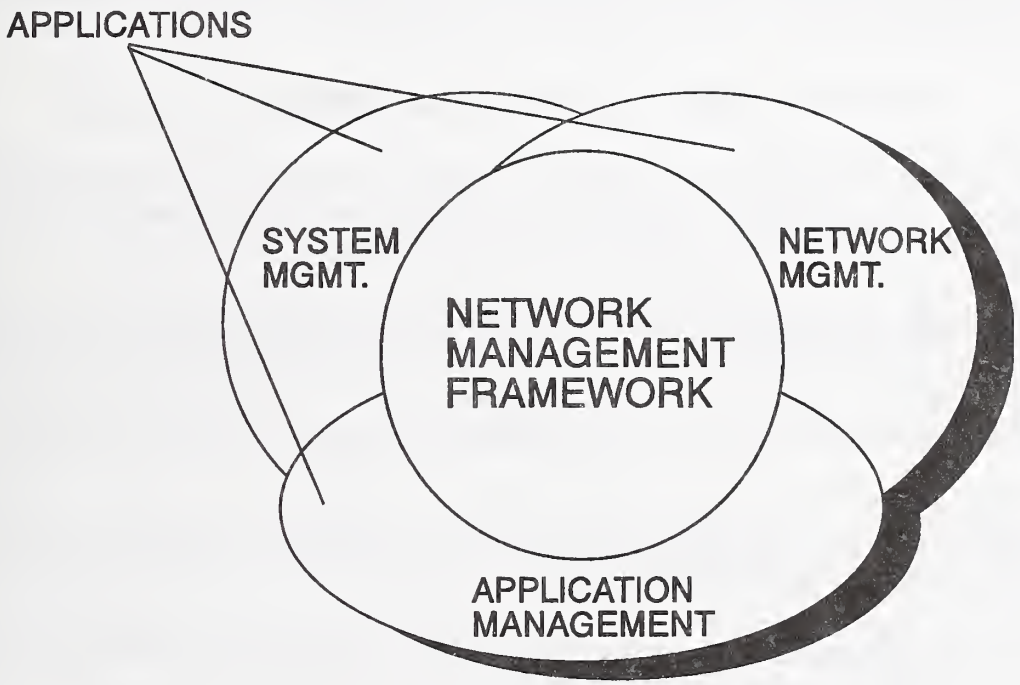

Figure 3. OSI Network Management Framework.

3.3.1 Operating System Services

Operating system services are the core services needed to operate and administer the application platform and provide an interface between application software and the platform. These core services consist of the following:

a) Kernel operations provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input-output processing to and from peripheral devices.

b) Commands and utilities include mechanisms for operations at the operator level, such as comparing, printing, and displaying file contents; editing files; pattern searching; evaluating expressions; logging messages; moving files between directories; sorting data; executing command scripts; and accessing environment information.

c) Realtime extension includes the application and operating system interfaces needed to support those application domains requiring deterministic execution, processing, and responsiveness. The extension defines the applications interface to basic system services for input/output, file system access, and process management.

d) System management includes capabilities to define and manage user resource allocation and access (i.e., what resources are managed and the classes of access defined), configuration and performance management of devices, file systems, administrative processes (job accounting), queues, machine/platform profiles, authorization of resource usage, and system backup.

3.3.2 Human/Computer Interface Services

Human/Computer Interface (HCI) services define the methods by which people may interact with an application. Depending on the capabilities required by users and the applications, these interfaces may include the following:

a) Client-server operations define the relationships between client and server processes operating within a network, in particular, graphical user interface display processes. In this case, the program that controls each display unit is a server process, whereas independent user programs are client processes that request display services from the server.

b) Object definition and management includes specifications that define characteristics of display elements: color, shape, size, movement, graphics context, user preferences, interactions among display elements, etc.

c) Window management specifications define how windows are created, moved, stored, retrieved, removed, and related to each other.

d) Dialogue support includes specifications that define the relationships between what is displayed on the screen (e.g., cursor movements, keyboard data entry, external data entry devices), and how the display changes depending on the data entered.

e) Multimedia specifications include API specifications, service definitions, and data formats that support the manipulation of multiple forms of digital and analog audiovisual data within a single application.

User interfaces are often the most complex part of system development and maintenance. Within the past few years, significant advances have been made in user interfaces technology in both ease-of-use and in reducing the development effort required.

The principal components of a window system are a video interface that contains one or more windows or panels; a pointing device such as a mouse or touch screen; and a set of objects on the screen that can be directly manipulated by the user through the pointing device or through keyboard responses.

Multimedia, in the art world, is the integration of two or more different modes of expression within a single work of art, such as the mixing of sculpture and music or painting and dance. In the world of information processing, multimedia is a general term that describes the integration of different information representations, such as text, sound, and video, within a single presentation session, especially within a common user interface. In addition to the traditional text and line graphics, multimedia applications often include scanned images, part- or full-motion video with or without synchronized audio, and digitized sound or music. Some of the key challenges in identifying and defining standards associated with this area include: analog to digital conversions, compression and storage of large data sets, synchronization of time-dependant representations, and multi-channel input and output.

3.3.3 Software Engineering Services

The production and use of portable, scalable, interoperable software is the objective of open systems. Software engineering services provide the infrastructure to develop and maintain software that exhibits the required characteristics. Standard programming languages and software engineering tools and environments become central to keeping with this objective. The required capabilities are provided by software engineering services which include the following:

a) Programming languages and language bindings for COBOL, FORTRAN, Ada, C, and Pascal.

b) Integrated software engineering environments (ISEE) and tools include systems and programs that assist in the automated development and maintenance of software. These include, but are not limited to, tools for requirements specification and analysis, for design work and analysis, for creating and testing program code, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various programs in the development environment.

3.3.4 Data Management Services

Central to most systems is the management of data that can be defined independent of the processes that create or use it, maintained indefinitely, and shared among many processes. Data management services include the following:

a) Data dictionary/directory services allow users and programmers to access and modify data about data (i.e., metadata). Such data may include internal and external formats, integrity and security rules, and be located within a distributed system.

b) Database management system (DBMS) services provide controlled access and modification of structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. DBMS services are accessible through a programming language interface or an interactive/fourth- generation language interface. For efficiency, database management systems generally provide specific services to create, populate, move, back up, restore, and archive databases, although some of these services could be provided by general file management capabilities described in operating system services.

c) Distributed data services provide access to, and modification of, data in a remote database.

3.3.5 Data Interchange Services

Data interchange services provide specialized support for the exchange of information, including format and semantics of data entities between applications on the same or different (heterogeneous) platforms. Data interchange services currently include the following:

a) Document services include specifications for encoding the data (e.g., text, pictures, numerics, special characters, etc.), and both the logical and visual structures of electronic documents.

b) Graphics data services include device independent definition of picture elements.

c) Product data interchange services encompass those specifications that describe technical drawings, documentation, and other data required for product design and manufacturing, including geometric and nongeometric data such as form features, tolerances, material properties, and surfaces.

LEVEL 5 — APPLICATION
LEVEL 4 — LANGUAGE SYNTAX AND SEMANTICS
LEVEL 3 — COMPLEX OBJECT
LEVEL 2 — OBJECT CONTENT
LEVEL 1 — DATA FORMAT

Figure 4. Data Interchange Complexity Levels.

There are various levels of complexity of data interchange. At the lowest level of complexity, Level 1, is the ability to define representations for the data to be interchanged. A representation might be defined as a language or a data format. The next higher level, Level 2, represents content. Text, raster images, and audio are examples of different content types. Level 3 includes object representations where different content types may be combined to form a complex data representation, such as a complex document. Above the object level is the language level, Level 4. The language level is suitable for humans to understand what is being represented. Level 5, the highest level of complexity, is the application level. The application level uses any of the lower levels of representation to interchange data with another application. Figure 4 illustrates the hierarchy among these levels of complexity.

3.3.6 Graphics Services

Graphics services provide functions required for creating and manipulating displayed images. These services include display element definition and management, and image attribute definition. The services are defined in specifications for describing multidimensional graphic objects and images in a form that is independent of devices. Graphics security services in this area include access to, and integrity of, functions that support the development of imaging and graphics software and image data.

3.3.7 Network Services

Network services provide the capabilities and mechanisms to support distributed applications requiring data access and applications interoperability in heterogeneous, networked environments. These services include the following:

a) Data communication includes API and protocol specifications for reliable, transparent, end-to-end data transmission across communications networks.

b) Transparent file access to available files located anywhere in a heterogeneous network.

c) Personal/micro computer support for interoperability with systems based on other operating systems, particularly microcomputer operating systems, that may not be formally standardized in a national or international standard.

d) Remote Procedure Call services include specifications for extending the local procedure call to a distributed environment.

3.3.8 Integral Supporting Services

Two supporting services are integrated within and permeate the other seven service areas. In many cases, separate specifications are not available for these supporting services within each of the seven service areas. These two services are security and management services described as follows.

3.3.8.1 Security Services

Security services are provided to support the secure distribution and integrity of information and to protect the computing infrastructure from unauthorized access. These services include the following:

a) Operating system security services specify the control of access to system data, functions, hardware, and software resources by users and user processes.

b) Human/computer interface security services include the definition and execution of types of user access to objects within the scope of human/computer interface systems, such as access to windows, menus, etc.; the functions that provide human/computer interface services such as human/computer interface management systems; and the security labeling of information on displays and other output devices.

c) Programming security services provide the means to control access to and integrity of programming objects such as libraries, program code, etc., and the tools or information that provide the infrastructure for development of software.

d) Data management security services include control of, access to, and integrity of data stored in a system through the use of specific mechanisms such as privileges, database views, assertions, user profiles, verification of data content, and data labels.

e) Data interchange security services are used to verify and validate the integrity of specific types of data interchange. Examples of such services include nonrepudiation, encryption, access, data security labeling, etc.

f) Graphics security services include those necessary to protect the integrity of and access to nontext data, such as graphical images (e.g., checksums on display bitmaps compared to file contents after encoding/decoding or compression/decompression techniques have been applied).

g) Network security services include access, authentication, confidentiality, integrity, and nonrepudiation controls and management of communications between senders and receivers of information in a network.

Individual security specifications are recommended within each of the other service areas. No specifications are defined in a separate security service area.

3.3.8.2 Management Services

Management services are integral to the operation of an open system environment. They provide the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components. Management services enable users and systems to become more efficient in performing

required work. Management is better able to streamline the operation, administration, and maintenance of open system components. These services include the following:

a) Fault management and control services that detect, log, and reconfigure systems through human intervention or through automatic means.

b) Configuration control services that provide mechanisms for performing version control.

c) Accounting services for monitoring system and network usage.

d) Performance monitoring services for computing effectiveness of configurations and estimating future performance requirements.

Individual management specifications are recommended within each of the other service areas. No specifications are defined in a separate management service area.

4. APP SPECIFICATIONS

Ideally, all specifications would be expressed in terms of international standards. Unfortunately, there are areas of OSE functionality for which formal standards, much less international standards, do not exist. Although this situation will improve over time, users who have requirements for those functions are faced with the question, "What specifications should I use now?"

4.1 Publicly Available Specifications

In some cases, there are no publicly available *open* specifications that pertain directly to a specific service area component. In those cases, NIST has tried to recommend a specification that at least partly covers the required functionality. In other cases, NIST has recommended specifications that are not entirely open, recognizing the fact that users need guidance now.

Publicly available specifications that may not be Federal standards can be used in some instances to fill the gaps between existing standards. NIST does not advocate that organizations should use the specifications in these cases without knowledge of the associated risks and adverse effects of such use (e.g., difficulty in porting applications later in a system's life, justifying the use of non-open specifications, etc.). If another specification appears to meet an organization's requirements more fully, then NIST recommends that the organization choose the one that meets those requirements the best. For a broad range of Federal applications and organizations, however, NIST can offer some insight into minimizing problems and managing those that cannot be solved directly at this time.

4.2 Specification Evaluation

The following sections describe the currently recommended specifications for each of the APP services and summarize some of the pros and cons of selecting each specification. The information is provided to managers, technical project leaders, and users to assist them in evaluating these specifications for inclusion in application or organizational profiles. These evaluations may be used to compare specifications listed in this guide to other specifications that an organization may be considering.

Each service area is preceded by a summary status report of all specifications reviewed in this report for that particular service area. An example of an entry from one of the summary status reports is presented in figure 5. Subsections of each service area describe specific evaluation criteria for the specification.

The summary status report relates the results of major evaluation criteria (e.g., level of consensus, completeness, etc.) to a graphic representation. With one view, all of the specifications in a particular service area can be compared to determine relative coverage of the area. Users may use this information to determine where they should concentrate their efforts in tailoring and augmenting application and organizational profiles.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
REALTIME IEEE P1003.4	O		O	●	O		

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

Figure 5. Example Summary Status Report.

4.3 Evaluation Criteria

Each of the specifications is evaluated according to how well it meets the requirements of a specific criterion. The criteria are defined as follows:

a) Level of consensus—A low evaluation is given to specifications that are proprietary or are used by a very limited or specialized group of users, such as vendor consortia; a high evaluation is given for a specification that has already become a national or international standard; average evaluations are assigned for public domain specifications that are not standard, or that may be in the process of becoming a standard (i.e., standards committee work-in-progress), or that are widely available across various hardware/software platforms.

b) Product availability—A low evaluation is given to specifications for which only a very few proprietary products are available; high evaluations are given to

specifications for which there is a wide variety of products available from various vendors across different application platforms; average evaluations are assigned to specifications that may be proprietary but have many products available from a variety of vendors, or that are public domain specifications with products readily available.

c) Completeness—A specification is evaluated on the degree to which it defines and covers key features necessary in supporting a specific functional area or service. For example a network security specification that includes all of the components described would be evaluated higher than others that do not include all of the features.

d) Maturity—According to the underlying technology of a specification, a high evaluation indicates that it is well-understood (e.g., a reference model is well-defined, appropriate concepts of the technology are in widespread use, the technology may have been in use for many years, a formal mathematical model is defined, etc.). A low evaluation indicates that it may be based on technology that has not been well-defined and may be relatively new.

e) Stability—A high evaluation means that the specification is very stable, that no changes are expected within the next 2 years. A low evaluation indicates that significant or many changes are expected within a relatively short time (1 to 2 years), or that incompatibilities exist between current and expected releases of the specification. An average evaluation is given to those specifications that may have known changes forthcoming to replace features in the existing specifications.

f) De facto usage—This evaluation criterion estimates the likelihood that a vendor will independently propose products that conform to this specification, whether or not a reference specification is stated in the procurement documents. A high evaluation indicates that most proposed products will conform to the specification. A low evaluation indicates that it is unlikely that the vendor will propose products based on the specifications. An average evaluation indicates that vendors are just as likely to propose products based on the specifications as not (i.e., no clear determination exists). In the cases of low or average evaluations, it is imperative that users include a specification in procurement documentation. A low evaluation does not necessarily mean that products implemented on the specification do not exist. It can also mean that some vendors would rather provide products that are not based on the recommended specifications, such as proprietary implementations.

g) Problems/limitations—Lower evaluations are assigned to specifications with severe restrictions on use or capabilities (e.g., licensing restrictions) or known problems tend to be to difficult and too numerous to overcome (e.g., new releases of the specification are not compatible with previous releases, or not enough is covered in the standard to be useful). An average evaluation is given to those specifications that require some minor additional facility in order to be fully effective in their intended environment. This additional facility may be provided by a related standard or other specification.

4.4 Additional Information on Specifications

Additional informational items, including the following, are provided where appropriate:

a) Specification title—The full identifying title of the specification for purposes of ordering or reference.

b) Specification available from—Organization from which the specification can be ordered.

c) Publication date—Date on which the publication was released for general use (usually designated on the specification's title page.)

d) Sponsoring organization—Organization responsible for developing and/or maintaining the specification. (In the case of certain Federal Information Processing Standards [FIPS] that adopt existing national or international standards, the organization responsible for the existing base standard is listed.)

e) Rationale—In a very few cases, a rationale section has been included to describe the reasoning behind a specific recommendation. The intent of this section is to show that a validation process was undertaken before a recommendation was made.

f) Applicability—Description of the OSE service area that covers the recommended specification.

g) Conformance testing—Provides information about current and future plans for conformance testing of products based on the recommended specification. In the case of FIPS testing, each FIPS PUB describes the requirements for testing and the policies that affect such testing. For other specifications, testing may or may not be described in the specification recommended.

h) Future plans—Published or otherwise-announced directions and long-term plans for individual specifications.

i) Alternative specifications—In some instances, other specifications exist besides the recommended specification. Users may want to review these alternatives before selecting a specification on which to standardize.

4.5 Federal Information Processing Standards

Federal Information Processing Standards (FIPS) are adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987. FIPS include standards, guidelines, and technical methods that are developed by NIST, approved by the Secretary of Commerce, and issued for governmentwide use.

FIPS frequently adopt standards that have been developed by national and international voluntary industry standards organizations with NIST assistance. This use of voluntary industry standards enables the Federal government to acquire commercially available off-the-shelf technology and to avoid the costs of developing its own standards.

NIST works with industry through voluntary standards committees and through sponsored activities such as the Open System Environment Implementors' Workshop (OIW) and the North American Integrated Services Digital Network User Forum (NIUF) to develop the technical agreements that are needed to implement standards in products.

The specific conditions under which standards are applicable to Federal government acquisitions are included in each FIPS. The extent to which each FIPS is compulsory and binding on Federal agencies is determined by the Secretary of Commerce when the FIPS is approved. Heads of agencies are authorized to waive the mandatory use of specific FIPS under certain conditions. Certain government systems are exempted from the use of the FIPS. These include classified computer systems and those that support specialized military and intelligence missions.

4.6 FIPS Testing

Each FIPS specifies whether testing is necessary to validate conformance of implementations. A test policy is produced by NIST/CSL for implementing the testing described. Each test policy is written to reflect the requirements of a specific FIPS. The testing policy defines what requirements must be met for testing, what test suites will be used, what procedures will be followed, and how test failures will be treated.

The National Voluntary Laboratory Accreditation Program (NVLAP), an organization within NIST, accredits laboratories for performing testing under various standards programs. The accreditation requirements are strict and differ for each standard. Accredited laboratories are generally reaccredited every 2 years.

A table of general conformance testing information is included for Federal Information Processing Standards that have associated test policies. Information for other specifications is included with the entry pertaining to the individual specification.

The specifications cited in Table 1 describe the types of testing specified in the FIPS. In some cases, a FIPS may describe optional levels that may be selected by organizations. Testing in such cases is also specified as optional within the FIPS. An organization may choose, however, to specify any level of testing for a particular acquisition.

If no failures are allowed by the specific FIPS testing procedures, an implementation cannot be validated as conforming if it fails any test. In some cases, validation can still occur even if test failures are allowed according to specific conditions defined within the testing policy associated with each FIPS. In such cases, mainly programming languages, an implementation must be revalidated within 12 months, and the same failures cannot reoccur.

Table 1. Summary of APP FIPS Conformance Testing Requirements

FIPS PUB	TEST AUTHORITY	TYPES OF VALIDATION
FIPS PUB 021-3 COBOL (Failures allowed)	NIST	Base/Registered
FIPS PUB 069-1 Fortran (Failures allowed)	NIST	Base/Registered
FIPS PUB 109 PASCAL (Failures allowed)	NIST	Base/Registered
FIPS PUB 119 Ada (Failures allowed)	AJPO	Base/Registered
FIPS PUB 120-1 GKS (No failures allowed)	NIST	Base
FIPS PUB 127-2 SQL (No failures allowed)	NIST	Base/Registered
FIPS PUB 128 CGM (No failures allowed)	NIST	Base
FIPS PUB 153 PHIGS (No failures allowed)	NIST	Base
FIPS PUB 146-1 GOSIP (Failures allowed)	NIST/JITC	Base/Registered
FIPS PUB 160 C (No failures allowed)	NIST	Base/Registered

The test authority column in Table 1 indicates the agency responsible for testing. POSIX testing is performed by NIST/NVLAP-accredited testing laboratories that submit test reports to NIST/CSL for review and final approval. In the case of Ada, the Ada Joint Program Office (AJPO) has testing authority and NIST/CSL is an Ada validation facility under the authority of the AJPO. NIST/CSL is the GOSIP test authority. The Department of Defense's Joint Interoperability Test Center (JITC) in Ft. Huachuca, Arizona, a NIST/NVLAP-accredited laboratory, performs testing and evaluation of GOSIP implementations for the U.S. Government and acts as NIST/CSL's agent for GOSIP validation. Other NIST/NVLAP-accredited laboratories also perform testing of GOSIP implementations, but the test results are reviewed by JITC for final approval.

There are three basic types of product validations:

1) Base validation denotes that a test was conducted using NIST-approved validation test suites and that the test was witnessed by accredited Government witnesses. A validation certificate or product registration is issued.

2) Registered validation indicates that an implementation with a base validation may have been minimally upgraded and tested on the same or a very similar platform, but without accredited Government witnesses present. The test results were then submitted to the testing authority for review. If the implementation passed the test, it is registered as a derived validation. No certificate is issued.

   Alternately, an implementation submitted for base validation may have failed one or more tests. In this case, the implementation is registered on the list of validated products, but no certificate is issued.

3) GOSIP implementations are registered in the same manner as base validations, but no certificates are issued. Instead, the implementation is registered on a public GOSIP validated products register. Note that there are individual tests for most protocols referenced in the GOSIP FIPS. This may result in multiple registrations for one product if it provides capabilities of multiple protocols. (A separate interoperability test is prescribed for GOSIP implementations. While such testing is strongly recommended, it is outside the scope of this report.)

4.7 Operating System Services

Operating system (OS) services include kernel operations, commands and utilities, system management, realtime extension, and security.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
FIPS PUB 151-2 POSIX	●	●	●	●	●	●	●
POSIX SHELL IEEE 1003.2-1992	O	●	●	●	●	●	●
REALTIME IEEE P1003.4	O		O	●	O		
SECURITY IEEE P1003.6				O			

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.7.1 Kernel Operations API

Specification title: FIPS PUB 151-2 Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]

Specification available from: National Technical Information Service (NTIS)

Publication date: April 1993

Sponsoring organization: The Institute of Electrical and Electronics Engineers, Inc. (IEEE)

Applicability: Kernel operations provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input-output processing to and from external devices. The FIPS is mandatory for use where POSIX-like requirements are defined.

Level of consensus: The U.S. Government's Federal Information Processing Standard Publication (FIPS PUB) is based on international standard ISO/IEC 9945-1:1990. The FIPS makes certain optional capabilities mandatory for Federal procurements.

Product availability: As of the date of this publication, there were over 100 products validated according to FIPS PUB 151-1 validation requirements on numerous types and classes of platforms. Validation for FIPS PUB 151-2 will begin as soon as testing laboratories are accredited to use the new test suite.

Completeness: The FIPS has undergone change to bring it in line with ISO/IEC 9945-1:1990. This standard does not, however, include other kernel operations that are widely understood as part of the operating system kernel, such as realtime operations or kernel security capabilities. These capabilities will become parts of related standards for augmenting the usability of FIPS PUB 151-2 in the future. For kernel operations, FIPS PUB 151-2 is complete as written.

Maturity: Antecedents of POSIX have existed for 20 years. The current standard was developed over a 10-year period. Much research based on POSIX antecedents has been pursued, which has led to various improvements in the POSIX specification.

Stability: FIPS PUB 151-1 adopted the 1988 IEEE POSIX standard. FIPS PUB 151-2 revises the previous FIPS to bring it into line with the current national (IEEE 1003.1-1990) and international (ISO/IEC 9945-1:1990) standards.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: POSIX consists of a family of related specifications, some of which are still in draft stages (e.g., IEEE P1003.4 Realtime Amendment, IEEE P1003.6 Security, etc.). FIPS PUB 151-2 is complete in itself. The other pieces mentioned herein will augment FIPS PUB 151-2 usability as additional FIPS PUBs.

Conformance testing: NIST has developed a conformance test suite and offers testing services via Accredited POSIX Testing Laboratories (APTL). Certificates of validation are issued by NIST. Validated products are listed in CSL's quarterly "Validated Products List" (VPL), on a NIST/CSL-supported E-mail server, and the NIST Gopher system.

Future plans: Existing kernel operations will not change, although additional operations are on the horizon. Related standards for other service area components, such as realtime operations, system security, etc., will be developed over the next 1 to 2 years.

Alternative specifications: None (All other known specifications that provide these services are compatible with POSIX.)

4.7.2 Operating System Commands and Utilities

Specification title: Planned FIPS PUB on Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities Interface IEEE Std 1003.2-1992, Information Technology—Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities

Specification available from: IEEE

Publication date: October 1992

Sponsoring organization: IEEE

Applicability: Commands and utilities include mechanisms for operations at the operator level, such as comparing, printing, and displaying file contents, editing files, pattern searching, evaluating expressions, logging messages, moving files between directories, sorting data, executing command scripts, scheduling signal execution processes, and accessing environment information. The shell programming language allows the creation of portable, easily-created scripts to perform actions that combine or tailor the functions performed by the individual utilities.

Level of consensus: The IEEE standard, IEEE Std 1003.2-1992 (POSIX.2), was approved in October 1992. The proposed FIPS will adopt POSIX.2 in its entirety. ISO/IEC 9945-2 has been proposed as an international standard and is expected to be adopted in mid to late 1993.

Product availability: Implementations of commands and utilities capabilities are available in proprietary operating systems that are very similar to the specification.

Completeness: The POSIX.2 Standard is currently complete. The POSIX.2b project, however, covers future extensions to POSIX.2 and new requests from other POSIX groups. The current draft of POSIX.2b, Draft 4-August 1992, includes changes to the archive format, the handling of symbolic links, a new conversion utility, and a number of other extensions.

Maturity: Antecedents and similarly specified implementations have existed for 10 to 20 years.

Stability: Significant new capabilities are expected to be added within the next 1 to 3 years, but should be compatible with the current standard.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that meet this specification, or that are compatible with the specification.

Known problems/limitations: None

Conformance testing: When a FIPS is adopted, NIST plans to provide certification procedures and tests for demonstrating product conformance. No time schedule has been developed for these actions, although the test assertions for POSIX.2 standard (IEEE POSIX 1003.3.2) is currently in ballot.

Future plans: The specification will be revised as needed to reflect the evolving national and international consensus.

Alternative specifications: UNIX International (UI) System V Interface Definition (SVID), Open Software Foundation OSF/1, X/Open Portability Guide Issue 4 (XPG4)

4.7.3 Operating System Realtime Services API

Specification title: Amendment 1: Realtime Extension [C Language] P1003.4 Draft 12

Specification available from: IEEE Working Group P1003.4

Publication date: February 1992

Sponsoring organization: IEEE

Applicability: Provides the operating system extensions needed to allow incorporation of realtime application domains into the OSE. The extensions define the applications interface to basic system services for input/output, file system access, and process management.

Level of consensus: P1003.4 is currently at Draft 12 and is in the balloting process.

Product availability: Implementations of some of these realtime extension capabilities are available in proprietary operating systems that are very similar to the specification. Many more are following suit even as the ballot process is undertaken.

Completeness: The functional specifications are still subject to modification, but major features are already included in the draft. The realtime extensions as currently defined are not complete. Fully-compliant implementations will begin to emerge as the draft matures.

Maturity: Commercially available operating systems are beginning to appear that contain some of the P1003.4 Draft functionality.

Stability: The specification is being balloted. There is a high probability that the ballot will succeed and document that consensus has been achieved.

De facto usage: The realtime extension and API for the most part can be expected to be available on most commercially available operating systems.

Known problems/limitations: The specification as it stands includes a C language binding (P1003.4) and the threads extensions (P1003.4a). Still to come are a language independent specification (LIS), realtime profiles, and testing specifications.

Conformance testing: When a FIPS is adopted, NIST plans to provide certification procedures and tests for demonstrating product conformance. No time schedule has been developed for these actions.

Future plans: Other related subparts and standards include: P1003.4b Operating System Interface, P1003.4c Language Independent Specification, and P1003.13 Realtime Profiles. P1003.4b and P1003.4c do not currently have scheduled ballot dates. Also, a related Draft P1003.13 (Realtime Profiles) has moved along rapidly and is currently in ballot resolution. As these specifications emerge they will be represented here.

Alternative specifications: None.

4.7.4 Operating System Security API

Specification title: Security Interface for the Portable Operating System for Computer Environments (IEEE P1003.6 Draft 11)

Specification available from: IEEE Working Group P1003.6

Publication date: July 11, 1991

Sponsoring organization: IEEE

Applicability: Security considerations are specified in terms of data encryption mechanisms, access control, reliability control, system logging, fault tolerance, and audit facilities. (The security interface does not specify a secure operating system; only its interface.)

Level of consensus: This specification is still in a draft stage and will probably be balloted in 1993.

Product availability: Implementations exist with the majority of defined features.

Completeness: Major topics including key features have not yet been finalized.

Maturity: The basic technology is well understood and the specification is based on several underlying standards/criteria.

Stability: With the expected balloting process to commence in 1993, consensus has evolved around the core document with minor exceptions. These exceptions may become options in the current document, or modifications in later versions. Resolution of ballots cast will determine the outcome.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: The specification is incomplete in some areas, most notably missing function and routine specifications that still have to be defined.

Conformance testing: A method of measuring conformance has not been defined. Until this has occurred, no determination of where or when testing might take place will be made. A set of draft test assertions has been developed for use in test suite development.

Future plans: Security specifications will expand to integrate interfaces for other service area components.

Alternative specifications: National Computer Security Center "Orange Book" security standards for access control (NCSC-STD-020-A) and password management (NCSC-STD-002-85); Defense Intelligence Agency (DIA) DRS-2600-5502-87: "Security Requirements for System High and Compartmented Mode Workstations (CMW);" DIA DDS-2600-6216-91: "Compartmented Mode Workstation Labeling: Encoding Format;" DIA DDS-2600-6215-91: "Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines"

4.8 Human/Computer Interface Services

The components of this service include the Graphical User Interface Service component, Planned FIPS PUB 158-1, which refers to the X Window System, version 11, release 5, and the Graphical User Interface Toolkit component.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
Proposed FIPS PUB 158-1 X Window System	●	O	O	●	●	●	
Draft Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (IEEE P1295.1)	●	●	O	O	O	●	O

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.8.1 Graphical User Interface API

Specification title: Proposed FIPS PUB 158-1 User Interface Component of Applications Portability Profile (MIT X Window System)

Specification available from: NTIS

Publication date: Announced October 20, 1992

Sponsoring organization: Massachusetts Institute of Technology X Consortium

Applicability: The MIT X Window System is the Federal standard for graphical user interfaces in the OSE. Its software, written in C, has proven to be highly portable between various hardware platforms and operating systems. Because of its client-server architecture, the X client application can run on one system while the X server can be running on another system on a network. As a result, networked PC's which run X server software can act as X terminals for X client applications running on OSE platforms.

Level of consensus: An X Protocol standard for constructing messages between clients and servers is being developed by Standards Committee X3K13.6; Xlib and the Xt Intrinsics (i.e., components for building GUI objects, such as push buttons, scroll bars, window borders, etc.) are not standardized at this time. An updated FIPS based on the X Consortium specifications described above has been proposed as FIPS PUB 158-1.

Product availability: Virtually all major hardware vendors have produced implementations of the X Window System for their product lines. A copy of the software is available from expo.lcs.mit.edu at Massachusetts Institute of Technology through the "ftp" command.

Completeness: The specification defines the primitives, intrinsic functions based on these primitives, and some of the lower level library specifications for human/computer interface services. It does not specify any of the "look and feel" or style services that will be accessible at higher levels of abstraction. It does not contain a full complement of utilities and services required to allow application programmers to easily program user interfaces.

The X Window System defines a C language source code level interface to a network-based bit-mapped graphic display system. The computer program source code contained in Version 11, Release 5, is not part of the specification for the FIPS. The specification for this FIPS includes the following documents from the X Consortium, X Window System, Version 11, Release 5:

1) X Window System Protocol, X Version 11
2) Xlib—C language X Interface
3) X Toolkit Intrinsics—C Language Interface
4) Bitmap Distribution Format 2.1.

Maturity: The X Window System has been in existence since 1983. It was one of the products to come out of Project Athena at MIT.

Stability: The Xlib, X Window System Protocol, and the Xt Intrinsics documents are stable. Further changes in these specifications are expected to include tuning modifications rather than major deletions or additions. A revised FIPS PUB will probably be issued when appropriate as other national and international standards are approved.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: Most of the functionality is available at a low level (i.e., too low for most application programming).

Conformance testing: The U.S. Government will accredit conformance testing services through the National Voluntary Laboratory Accreditation Program (NVLAP) when test suites and testing policy for Planned FIPS PUB 158-1 become available.

Future plans: Revision of the FIPS will be considered and made where appropriate as national and international standards are approved. IEEE Working Group P1201 is preparing two documents: IEEE P1201.1 focuses on a high-level window application program interface toolkit; IEEE P1201.2 is concerned with drivability/usability of human/computer interfaces. The Inter-Client Communications Conventions Manual (ICCCM) from the MIT X Consortium, which defines how user application programs communicate with each other in a system, will be included in a future update of FIPS PUB 158.

Alternative specifications: None

4.8.2 Graphical User Interface Toolkit API

Specification title: Draft Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (IEEE P1295.1)

Specification available from: IEEE Working Group P1295.1

Publication date: N/A

Sponsoring organization: IEEE

Applicability: This specification supports writing portable applications with graphical user interfaces based on the X Window System. It defines a source code level interface to an X Window System toolkit graphical user interface environment based on the OSF MOTIF Application Environment Specification User Environment Volume. It includes a C language application program interface that is consistent with the Graphical User Interface Drivability Recommended Practice developed by IEEE P1202.2.

NOTE: IEEE P1201.1, Draft Standard for Information Technology—Uniform Application Program Interface—Graphical User Interface, is an upcoming specification that may accommodate a broad range of proprietary and non-X-Window-System-based GUI technologies within a single API. The P1201.1 Working Group plans to complete a draft document suitable for evaluation in late 1993.

Level of consensus: The IEEE P1295.1 Working Group has advanced the toolkit API based on OSF MOTIF. The technical credibility and maturity of the specification is reflected by the successful, large installed base of technology which complies with the specification. It is scheduled to be in the ballot process by the time this publication is available. Due to the substantial consensus already achieved in the industry, NIST expects this specification to move from a de facto to a de jure status in a relatively short time.

Product availability: Virtually all POSIX platform vendors and users are already using implementations of MOTIF from which the P1295.1 specification was derived.

Completeness: The P1295.1 specification provides a toolkit of functions and objects for developing application interfaces for GUI. Use of the P1295.1 specification in conjunction with FIPS PUB 158 implementations of the X Window System will provide a complete GUI, but without management capabilities that can be provided in dialog and presentation tools such as user interface management systems (UIMS).

Maturity: Existing applications that are written to comply with the OSF MOTIF API specification should port easily to the P1295.1 specification.

Stability: Due to industry committment to a substantial installed base, the specification should remain stable. Extensions to the Graphical User Interface Toolkit specification may be proposed within 1 to 2 years. Consensus is converging rapidly on the P1295.1 specification.

De facto usage: If users do not reference the P1295.1 specification in procurement documents, vendors will probably propose products that meet this specification or that are compatible with this specification.

Known problems/limitations: The P1295.1 specification provides only the toolkit level interface. An underlying GUI system, such as the X Window System, must also be provided to complete the GUI.

Conformance testing: No conformance tests exist. Plans for testing are being considered by the Working Group.

Future plans: Presentation and dialog management services will be defined after the toolkit specification is adopted.

Alternative specifications: None.

4.9 Software Engineering Services

Programming languages, language bindings, Integrated Software Engineering Environments (ISEE), and software engineering tools are included as components of software engineering services. The programming languages included herein are broad-based FIPS programming languages. While other programming languages are developing (e.g., C++, LISP, and Prolog), or may be specified as FIPS (e.g., MUMPS and BASIC), no

attempt to include every programming language was made. As consensus develops and needs warrant, each language will be considered for inclusion as a recommended specification within the APP. (Alternative specifications are not included for programming languages.)

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
FIPS PUB 119 Ada	●	●	●	●	●	●	●
FIPS PUB 160 C	●	●	●	●	●	●	●
FIPS PUB 21-3 COBOL	●	●	●	●	●	●	●
FIPS PUB 69-1 FORTRAN	●	●	●	●	●	●	●
FIPS PUB 109 Pascal	●	●		●	●		
ECMA PCTE	●			○	○		

Legend: ●-high evaluation ○-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.9.1 Programming Language Ada

Specification title: FIPS PUB 119 Ada

Specification available from: NTIS

Publication date: November 8, 1985

Sponsoring organization: Ada Joint Program Office

Applicability: Ada is a general-purpose, high-level programming language. In addition, it provides strong data-typing, concurrence, and significant code-structuring capabilities. It is particularly suited to embedded realtime systems, distributed systems, highly reliable software development, and reuse of proven code.

Level of consensus: Ada is a national standard (ANSI/MIL-STD-1815A-1983), an international standard (ISO 8652:1987), and a FIPS. The Department of Defense has directed that Ada be used in all DoD systems development.

Product availability: Numerous DoD-validated compilers and Ada environments are available commercially.

Completeness: Ada is complete for use as a general-purpose programming language.

Maturity: Ada was developed as a DoD-sponsored language and is based on well-defined predecessor languages such as Pascal.

Stability: Ada has the backing of the Department of Defense, the U.S. Government, the American National Standards Institute (ANSI), and the International Organization for Standardization (ISO).

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: Insofar as the majority of POSIX bindings are written in C, specialized standards groups are working on Ada bindings. Generally, there are few standardized bindings for Ada.

Conformance testing: Ada conformance and validation testing are carried out under the auspices of DoD's Ada Joint Program Office (AJPO). A monthly list of validated compilers is published by AJPO. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations. An additional compiler performance measurement testing service is available through AJPO.

Future plans: A new revision of Ada (a.k.a. Ada-9X) is in the review process and is planned for release in 1993. Related standards are in the process of adding, or have added Ada bindings (e.g., SQL [Planned FIPS PUB 127-2]. A new standard binding for Ada/POSIX kernel operations, IEEE 1003.5, was recently adopted by IEEE. The FIPS PUB will be revised to reflect the Ada-9X standard. A test suite for Ada-9X should be available several months after adoption of the Ada-9X standard.

4.9.2 Programming Language C

Specification title: FIPS PUB 160 C

Specification available from: NTIS

Publication date: March 13, 1991

Sponsoring organization: Standards Committee X3J11

Applicability: C is a general purpose high-level programming language designed for use in various levels of software including operating systems, system level software (e.g., special purpose processors), and business and scientific application software.

Level of consensus: FIPS PUB 160 and the ANSI standard are based on the International Standard, ANSI/ISO 9899:1992. FIPS PUB 160 specifies certain options and minimum capabilities that are left as options or variables within the ANSI standard.

Product availability: Numerous ANSI C compilers, interpreters, and associated products are commercially available and supported. Many of the compilers are also FIPS-validated and are commercially available.

Completeness: C includes facilities for every level of programming, from low-level (hardware control) operations to high-level abstract functions and procedures. Data structuring, reusable library support, and memory management are included.

Maturity: Development of C has progressed from a family tree of similar languages developed in academia, to a well-defined, widely supported language over a period of 15 years.

Stability: Standards Committee X3J16 is considering changes to fine-tune the standard based on usage experience.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: C does not provide direct support for data abstraction, information hiding, inheritance, or operator overloading. A new standard is developing to incorporate these capabilities within the C programming environment (see Future Plans below.)

Conformance testing: The U.S. Government established testing procedures and a testing service in August 1992 for formal validation using the FIPS. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Future plans: Standards Committee X3J16 is developing the C++ language standard, which will provide the tools for object-oriented software development. A working draft document is expected to be available for review in September 1994.

4.9.3 Programming Language COBOL

Specification title: FIPS PUB 21-3 COBOL

Specification available from: NTIS

Publication date: January 12, 1990

Sponsoring organization: Standards Committee X3J4

Applicability: COBOL is designed for use in programming self-documenting business oriented applications.

Level of consensus: The FIPS and international standards (ISO 1989:1985) are based on ANSI Standard X3.23-1985 and Addendum X3.23A-1989.

Product availability: COBOL is the most widespread programming language. An overwhelming percentage of all existing Federal applications are written and maintained in COBOL. All major vendors offer FIPS COBOL.

Completeness: The current standard does not include realtime, operating system, and communications components. It is most complete in the areas of data manipulation, and business/financial applications, which is its intended domain.

Maturity: COBOL is one of the oldest standard general-purpose programming languages, having been established in the early 1960's by DoD initiative.

Stability: The X3J4 Standards Committee is in the process of adding new functionality for communications interfaces and screen management. Compatibility with previous versions of the standard will be maintained. This has historically been one of COBOL's stronger points.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: COBOL has always been specialized toward the development of general-purpose business and financial applications. It is limited in other types of application domains, such as in realtime and communications, although this may change with functionality introduced by proposed revisions.

Conformance testing: FIPS conformance test suites are available from Federal sources. Testing services are also available from NIST. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Future plans: The addition of new functionality over the next 3 to 5 years will greatly expand the capabilities of COBOL to other application areas. An example of expansion includes object-oriented capabilities.

4.9.4 Programming Language Fortran

Specification title: FIPS PUB 69-1 Fortran

Specification available from: NTIS

Publication date: December 24, 1985

Sponsoring organization: Standards Committee X3J3

Applicability: Fortran is a high-level programming language used largely in scientific and engineering applications where large amounts of data are analyzed and processed in computationally intensive environments.

Level of consensus: The FIPS and the international standard (ISO 1539:1980) are based on the national standard (ANSI Standard X3.9-1978).

Product availability: Every major hardware vendor markets a Fortran compiler based on the standard. Additional compilers are available from a multitude of software vendors.

Completeness: It is a general-purpose programming language with capabilities for performing virtually any type of application function. It was originally developed to assist in the development of scientific calculation applications, but it has since been extended to cover other types of applications.

Maturity: Fortran is one of the oldest programming languages and was also the first one to be standardized.

Stability: Although it has undergone several major revisions over its lifespan, Fortran contains virtually all of the same capabilities that were available when it was new. In addition, it contains elements for assisting in the development of information systems, realtime and process control systems, structured programming constructs, etc.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: Due to loose data-typing and some idiosyncracies of various compilers, some debugging problems are very difficult to locate and fix.

Conformance testing: Conformance test suites are available from Federal sources. Testing services are also available from NIST. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Future plans: An IEEE Working Group is defining a POSIX/Fortran binding.

4.9.5 Programming Language Pascal

Specification title: FIPS PUB 109 Pascal

Specification available from: NTIS

Publication date: January 16, 1985

Sponsoring organization: Joint ANSI X3J9-IEEE Pascal Standards Committee

Applicability: Pascal is a high-level programming language used primarily in teaching environments for training computer science students in the concepts of programming. It is also used in general application areas such as business, science, etc.

Level of consensus: The FIPS and international standard (ISO 7185:1983) are based on the national standard (ANSI/IEEE770X3.97-1983).

Product availability: Numerous hardware and software vendors market standard implementations of Pascal interpreters and compilers.

Completeness: Pascal is a general-purpose programming language. It does not presently have constructs for performing file input-output at other than the byte level.

Maturity: Pascal is a strongly typed language based upon a model of program design that is well understood, and has been used extensively for teaching programming in universities.

Stability: Extended Pascal was adopted in 1990, but is not scheduled to become a FIPS. Stability of the current FIPS is not in question.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: FIPS Pascal does not have well-developed intrinsic file input-output operations.

Conformance testing: Conformance test suites are available from commercial sources, and testing services are available from NIST. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Future plans: NIST is currently considering whether to discontinue validating Pascal compilers based on the low need of this language by Federal agencies and the limited resources that NIST has for validation efforts. No initiatives are underway to make Extended Pascal a FIPS.

4.9.6 Integrated Software Engineering Environment

Specification title: Portable Common Tools Environment (PCTE): Abstract Specification, Standard ECMA-149, European Computer Manufacturers Association (ECMA)

Specification available from: ECMA

Publication date: December 1990

Sponsoring organization: ECMA Technical Committee 33 (ECMA/TC33)

Rationale: NIST is working to develop a suite of standards in the ISEE area and has incorporated the ECMA reference model in the base definition for the ISEE framework functionality, technical integration, and standards specification. The ECMA reference model is used to identify the needed functionality from which a comprehensive set of

services, interfaces, and data formats for integrating software tools can be developed. A cornerstone for the interoperability of software engineering tools within ISEE environments is the existence of a framework which provides a consistent set of services to allow for the integration of data, control, and presentation attributes among the various tools in the environment. PCTE is one such open standard that provides for some of these framework services, principally in the data repository area.

Applicability: Integrated software engineering environments (ISEE) and tools include systems and programs that assist in the automated development and maintenance of software. These include, but are not limited to, tools for requirements specification and analysis, for design work and analysis, for creating and testing program code, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various programs in the development environment. PCTE can provide for this data repository functionality.

Level of consensus: PCTE has a fair degree of consensus among major European manufacturers, and ECMA has planned to submit PCTE for ISO standardization in the near future. Some U.S. companies have announced plans to develop PCTE technology, although no firm product release dates have been announced.

Product availability: No product implementing full ECMA PCTE compliance is now available, although products implementing a subset of ECMA PCTE are expected in 1993. There are several implementations of the earlier PCTE 1.5 specification, which is a subset of the currently specified PCTE functionality. The earlier versions are not strictly compatible with the full standard.

Completeness: ECMA/TC33 plans to make slight modifications to the ECMA-149 standard in 1993 before it submits the standard for ISO adoption. There has been some concern voiced that PCTE will not execute efficiently with systems built using object-oriented design techniques due to what appears to be inherent inefficiencies in handling small data objects. Various groups (ECMA/TC33, the North American PCTE Users Group [NAPUG], and the North American PCTE Initiative [NAPI]) have started to look at evolving the standard to resolve this issue.

Maturity: PCTE has been under development since 1982, and under ECMA sponsorship since 1988. The basis entity-relationship (ER) data repository model used by PCTE is fairly stable and unlikely to undergo major changes in the future. Enhancements to address object-oriented design and further developments to aid data, control, and presentation integration are all possible in the future.

Stability: ECMA PCTE is still very much a new specification, and enhancements or modifications are to be expected. The emergence of products implementing the full standard in the next 2 years will undoubtedly indicate areas where the standard needs to undergo evolution.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: The current PCTE specification can accommodate the representation of large data objects, such as documents, but does not provide an efficient mechanism for representing small objects, such as data elements and the associated actions. The lack of products implementing the full standard makes it impossible to test and evaluate the full standard.

Conformance testing: The new NAPI organization formed by DoD, NIST, and the Object Management Group (OMG) has as one of its goals the development of a conformance test suite. The completion of this test suite, however, is probably several years off.

Future plans: NIST is one of the participants in NAPI with the objective to develop a conformance test suite and to aid in the evolution of the PCTE standard. A language binding for C++, in addition to the current C and Ada bindings, is now under development.

4.10 Data Management Services

Data management services include the data dictionary/directory component for accessing and modifying data about data (i.e., metadata), the database management system component for accessing and modifying structured data, and the distributed data component for accessing and modifying data from a remote database.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
Planned FIPS PUB 127-1 SQL	●	●	●	●	●	●	●
FIPS PUB 156 IRDS	O		●	●	O		
RDA	O		O		O		O

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.10.1 Relational Database Management System Interface

Specification title: Planned FIPS PUB 127-2 Database Language SQL

Specification available from: NTIS

Publication date: Expected mid-1993

Sponsoring organization: Standards Committee X3H2

Applicability: FIPS SQL provides data management services for definition, query, update, administration, and security of structured data stored in a relational database. A relational database is appropriate for general purpose data management, especially applications requiring flexibility in data structures and access paths; it is particularly desirable where there is a substantial need for *ad hoc* data manipulation or data restructuring. The security interface for granting and revoking privileges does not specify a secure DBMS; only its interface.

Level of consensus: Planned FIPS PUB 127-2 adopts ANSI Standard X3.135-1992 (SQL), which is identical to ISO/IEC Standard 9075:1992. SQL has been adopted as the database management component by X/Open, OSF, SQL Access Group, and other vendor consortia.

Product availability: Numerous implementations of the original ANSI SQL exist on all classes and brands of platforms. The NIST SQL Validated Products List maintains a long list of validated products and environments that conform to the earlier FIPS PUB. Vendors are vigorously implementing the additional features of the new ANSI SQL as specified in Planned FIPS PUB 127-2. In addition, vendors provide proprietary extensions to the standard as a mechanism for adding value. These extensions may not be compatible with future directions that the standard may take.

Completeness: The new SQL standard specifies data definition, view definition, access control, integrity constraints, schema manipulation, data manipulation (Select, Insert, Update, Delete), Dynamic SQL, transaction management, connection management, session management, diagnostics management, information schema tables, and two methods of programming language bindings (Module and Embedded) for seven different programming languages (Ada, C, COBOL, Fortran, MUMPS, Pascal, and PL/I). FIPS SQL requires ANSI Standard X3.135-1992 Entry SQL conformance to one or more FIPS programming languages and requires a FIPS Flagger to flag extensions in an implementation. FIPS SQL provides options for three other levels of conformance (Transitional, Intermediate, and Full), specifies character sets and a documentation schema required to be supported in FIPS Intermediate SQL and above, and specifies default SQL sizing requirements. The FIPS provides options for SQL interoperability using the Remote Database Access (RDA) SQL Specialization. The FIPS also contains specifications for some Discretionary Access Control (DAC) mechanisms, but not Mandatory Access Control (MAC) nor the associated security labels. For a definition of DAC or MAC, refer to "Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria" (NCSC-TG-021 Version 1, "Lavender Book"), National Computer Security Center, April 1991.

Maturity: The SQL data model is based on the relational model first published in 1969. The first commercial systems were available in 1979, and the first SQL standard was published in 1986. All subsequent standards have been upward compatible enhancements to add new facilities and features.

Stability: The SQL language has firm mathematical foundations in the first-order predicate calculus. Standards groups and vendors are firmly committed to upward compatibility in revisions and future extensions to the standard. Existing features are expected to remain stable for the foreseeable future.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: The existing standard is a nonprocedural data manipulation language. It applies to stand-alone, single-environment database architectures. It also applies to client-server architectures with proprietary internal interfaces and protocols. When combined with the RDA standard in Section 4.10.3, SQL is suitable for heterogeneous distributed database processing. Enhancements are under development to provide user-defined data types, triggers, assertions, flow of control statements, and other capabilities associated with object data management.

Conformance testing: A formal SQL test service was instituted by NIST in April 1990 and currently uses Version 3.0 of the NIST SQL test suite. Version 3.0 has been publicly available since January 1992. The SQL test suite measures conformance to both required and optional features of Planned FIPS PUB 127-1. NIST publishes a quarterly list of FIPS-validated processors. Certificates of validation are issued for products tested that show fully conforming test results. Validation summary reports (VSR) are issued for each test conducted, regardless of whether products have nonconformities. Version 4.0 of the NIST SQL test suite, to test required features of the new FIPS SQL standard, is expected in mid-1993.

Future plans: Specifications for SQL interoperability with remote heterogeneous sites are under development in an emerging ISO/IEC Remote Database Access (RDA) standard (see sec. 4.10.3). An SQL Call Level Interface (SQL/CLI), to provide a services interface for third-party software vendors, and a specification for Persistent SQL Modules, to allow interchange of complete SQL stored procedures, are both under development with completion expected early in 1995. An emerging SQL3 specification, with features for managing complex objects in heterogeneous environments, is under development in ANSI and ISO standardization committees, with completion expected in the 1996 time frame. The SQL3 specification will include triggers, assertions, user-defined data types, object hierarchies, inheritance, and other features for management of complex objects. A new project for development of SQL Multimedia and other Application Packages (SQL/MM) is under ballot with completion of initial parts for Full-Text, Images, and Spatial Data projected for completion in 1996. Revised FIPS SQL standards that adopt the new SQL enhancements are expected as appropriate.

Alternative specifications: None.

4.10.2 Data Dictionary/Directory System

Specification title: FIPS PUB 156 Information Resource Dictionary System (IRDS)

Specification available from: NTIS

Publication date: April 5, 1989

Sponsoring organization: Standards Committee X3H4

Applicability: Data dictionary/directory services consist of utilities and systems necessary to catalog, document, manage, and use metadata (information about data).

Level of consensus: ANSI Standard X3.138-1988 and the FIPS are the same document. ISO has completed an IRDS specification that is significantly different in some respects from the ANSI standard.

Product availability: Commercial implementations have been developed, but their quality has not yet been determined. A prototype implementation is available from CSL which contains a large subset of IRDS functionality.

Completeness: The FIPS specification includes human/computer interfaces only. ANSI Standard X3.185-1992, IRDS Services Interface, provides an application program interface to the IRDS. It is appropriate for metadata interchange with a database management system, and between an IRDS and application programs. ANSI Standard X3.195-1991, IRDS Export-Import File Format, supports schema and metadata interchange among IRDS-compliant databases, among IRDS and CASE tools with repositories or dictionaries, between IRDSes and application programs, and between other systems that wish to employ the exchange mechanism that it specifies.

Maturity: Antecedents of the IRDS have been in existence for 15 years. The current specification has been in development during the major part of this time.

Stability: The next 2 to 3 years should see nominal changes in the current standard. Related standards efforts are specifying additional and upwardly compatible functionality.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: Virtually all procurements that specify a data dictionary/repository require it to be active. In such cases, the FIPS PUB 156 IRDS would need to be augmented by the ANSI standard, X3.185-1992, discussed above.

Conformance testing: Conformance tests for FIPS PUB 156 are currently under development.

Future Plans: Related standards work will provide additional functionality and capability to manage object-oriented data structures and provide for enhanced communication of information between applications and other data management tools. A major revision to the standard is envisioned in about 3 years to include this new functionality.

Alternative specifications: None.

4.10.3 Distributed Data Access

Specification title: Remote Database Access (RDA) ISO/IEC 9579:1993

Specification available from: ANSI

Publication date: Expected Early 1993

Sponsoring organization: ISO/IEC JTC1

Applicability: RDA is used to establish a remote connection between an RDA client, acting on behalf of an application program or a client data manager, and an RDA server, interfacing to a process that controls data transfers to and from a database. The goal is to promote the interconnection of applications and the interoperability of database management systems among heterogeneous environments.

Level of consensus: The ISO/IEC RDA specification was completed by the ISO technical development committee in June 1992 and formal ISO/IEC approval is expected in early 1993. The specification is in two parts: Part 1 -- Generic Model, Service, and Protocol, and Part 2 -- SQL Specialization. RDA is a working task group of the NIST Open System Environment Implementor's Workshop (OIW) and RDA agreements for the Basic Application Context of the SQL Specialization are part of the December 1992 Stable Agreements. Agreements for the Transaction Processing (TP) Application Context are under development in OIW. RDA will also be included in GOSIP version 3.

Product availability: Vendor consortia such as the SQL Access Group have demonstrated interoperability with working prototypes among different SQL servers. Many SQL vendors are planning to have conforming client and server products available soon after formal adoption of RDA by ISO/IEC in 1993.

Completeness: RDA services consist of dialogue management, association control, resource handling, and data language services between a single client and a single server. Association control includes making a connection to a specific database at the server site. SQL statements are sent as character strings with a separate list of input parameters, and resulting data or exception conditions are returned. Transaction management services are also included for both one-phase and two-phase commit protocols. Different application contexts are negotiable to determine whether one-phase (Basic context) or two-phase commit (TP context) are available. The existing specification does not consider integrated concurrency control mechanisms, so distributed database management is the concern of

the client process. Extensions for true distributed database management among different SQL implementations are under consideration.

Maturity: Methods for establishing communications links between client and server sites are well known, but agreements on nonproprietary communications protocols are very new.

Stability: The client-server architecture is just one of several architectures used for implementing distributed systems and there is no final conclusion as to which is best. The stability of RDA depends on the stability of the client-server architecture.

De facto usage: If users do not reference this specification in procurement documents, some vendors will propose products that meet this specification, and other vendors will propose products that do not meet this specification.

Known problems/limitations: The RDA SQL Specialization only supports Entry SQL from the SQL-1992 standard. Support for features in Intermediate SQL and Full SQL are under development with approval expected in 1994. Although distributed extensions are under consideration, RDA does not currently specify distributed database, except what is achievable by the client using two-phase commit protocols among different servers.

Conformance testing: RDA will likely become a future part of conformance testing for GOSIP. At the present time, RDA can be tested indirectly using the NIST SQL test suite, with application programs at the client site and data at the server site.

Future plans: Enhancement projects for distributed database and stored database procedures have already been proposed to ISO. Extensions to support new features in the recently adopted SQL-1992 standard are under development. Vendor agreements reached by various consortia are finding their way into the RDA standard.

Alternative specifications: None.

4.11 Data Interchange Services

Data interchange services provide specialized support for the exchange of information, including format and semantics of data entities, between applications on the same (homogeneous) or different (heterogeneous) platforms.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
ODA/ODIF/ODL ISO 8613	●		●	O	O		O
FIPS PUB 152 SGML	●		O	●	●		O
SPDL ISO 10180	●		●	●	●		●
EMPM ANSI/NISO Z39.59	●	O	●	●	●		O
FIPS PUB 161 EDI	●	●	●	●	O	●	O
FIPS PUB 128 CGM	●	●	●	●	●	●	●
FIPS PUB 177 IGES	●	●		O	●	●	●
STEP ISO 10303			●	●			
FIPS PUB 173 SDTS	O	O	●	●	●	●	●

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.11.1 Document Interchange

Specification title: Open Document Architecture/Open Document Interchange Format/Open Document Language (ODA/ODIF/ODL) ISO 8613:1989

Specification available from: ANSI

Publication date: May 1989

Sponsoring organization: ISO/IEC JTC1, CCITT

Applicability: Open Document Architecture (ODA) is a framework that enables users to interchange the logical structure, content, presentation style and layout structure (the physical appearance) of documents from one application to another, or from an application to various output devices. ODIF, Open Document Interchange Format, is an ASN.1 (Abstract Syntax Notation One--ISO 8824:1987 and ISO 8825:1987) encoding for documents suitable for interchange between applications. ODL, Open Document Language, is a generic Standard Generalized Markup Language (SGML) encoding for documents suitable for interchange between applications. ODA/ODIF/ODL can represent

complex objects that include different types of contents, such as complex documents with embedded text, graphic images, etc. Typical uses of ODA/ODIF might include transmitting formatted documents, such as books and technical reports through communications networks from one application to another and then printing or editing the file through various filters (e.g., a text filter, a graphics filter, or a printer driver). An ODA/ODIF encoded file can be a bitmap representation, a text character representation, or a combination of these and other representations. The physical appearance of the document will normally be maintained throughout the operations of encoding, transmitting, and unencoding. Specific Document Application Profile (DAP) encodings are required to make efficient use of ODA/ODIF, but they are not described or recommended in the APP. Users should consult with experts in ODA/ODIF capabilities.

Level of consensus: The international standard (ISO 8613) was approved by two international standards bodies, ISO and International Telegraph and Telephone Consultative Committee (CCITT). Additionally ODA has been adopted for the encoding of tiled raster images by the Department of Defense in the Computer-Aided Acquisition and Logistics Support (CALS) initiative as described in MIL-R-28002B.

Product availability: A few vendors are implementing a major subset of ODA (Level 2 in the specification) using ODIF as an interchange format.

Completeness: ODA/ODIF/ODL covers all aspects of document interchange, including logical structure, layout structure, generic logical structure, generic layout structure, and presentation. Documents can be interchanged in either a processable, formatted, or a mixed processable formatted form. A Document Application Profile (DAP) is also required to interchange a document between applications. A DAP defines the environment for combining the various complex parts of an ODA/ODIF encoded document and how this document is to be treated in various contexts, such as printing or editing.

Maturity: The connection between document logical structure, layout, and content is still an active topic of research.

Stability: Minor revisions of the standard will be made as vendors develop implementations.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: A complex document can be encoded using ODA/ODIF, but the specifications of individual encoding schemes and document structures are very low-level. A Document Application Profile (DAP) is recommended for specifying more abstract structuring in a document.

Conformance testing: NIST is developing a plan for conformance testing. The Department of Communications (Canada) and the NCC (UK) have test-suite developments underway.

Future plans: A FIPS to adopt ISO 8613:1989 is planned within the next year.

Alternative specifications: Electronic Manuscript Preparation and Markup, standard ANSI/NISO Z39.59-1988, is an alternative national standard for representing the logical structure of books, articles, and serials. Several organizations have designed alternative nonproprietary architectures with SGML encodings. Those organizations are the Association of American Publishers (AAP), the Text Encoding Initiative (TEI), and the Department of Defense CALS program. Many vendors still recommend that organizations require unique nonstandard document architectures encoded in SGML.

4.11.2 Document Interchange

Specification title: FIPS PUB 152 Standard Generalized Markup Language (SGML)

Specification available from: NTIS, ANSI, GCA

Publication date: September 26, 1988

Sponsoring organization: ISO/IEC JTC1

Applicability: Interchange of documents — SGML is intended to formally define the grammar of languages for document markup. It provides a means to specify what markup is allowed, what markup is required, and how markup is distinguished from text.

Level of consensus: SGML is defined by international standard ANSI/ISO 8879:1986. The FIPS specifies a profile of capabilities that are defined in the ANSI/ISO standard and sets minimum options for use in Federal systems.

Product availability: Several implementations that use SGML encodings to parse their input are available from vendors. More implementations are in development.

Completeness: A high percentage of SGML features are available in current implementations. SGML does not deal with the meaning of the markup. (Markup consists of the common sets of document formatting codes used in classes of document types. For example, technical manuals may use a different markup from management guideline documents due to the audience and content of the respective document types, and the types of publishing layouts that are commonly used for each.) Therefore SGML does not specify what to do after the document has been processed by an SGML-recognizing program.

Maturity: The technology upon which SGML is based has existed for at least 7 years. Precursors of SGML include Backus Naur Form, Regular, Context Free, Left-to-Right scanning with k-token lookahead (LR[k]), and Context Sensitive grammars. These are well understood and have a rich mathematical basis.

Stability: The position as a grammar representation standard makes SGML a very stable specification. It is generalized to the extent that various other representations and models

can be included and represented within the SGML framework. The market is having difficulty, however, adopting any of the many possible SGML-encoded markup architectures as a basis for interchange. See Known problems/limitations.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or are not compatible with the specification.

Known problems/limitations: While consensus on the SGML standard has been reached to some degree, there is still a great deal of disagreement on particular markup to be employed. The APP recommends at least one specification for defining markup: Electronic Manuscript Preparation and Markup (see sec. 4.11.4).

Conformance testing: The Graphics Communication Association (GCA) is discussing plans to produce a conformance test suite. A prototype test suite has been developed by NIST.

Future plans: SGML is currently being reviewed by ISO and proposals for enhancements may be put forward over the next 1 to 3 years. The standards developers have agreed that any future changes will not affect existing conforming SGML documents.

Alternative specifications: ODA/ODIF/ODL ISO 8613:1989

4.11.3 Page Description Language

Specification title: Planned FIPS for Standard Page Description Language (SPDL) ISO/IEC DIS 10180

Specification available from: ANSI

Publication date: April 18, 1991

Sponsoring organization: Standards Committee X3V1.8

Applicability: SPDL defines a language for representing images that are to be displayed on a screen, printed on an output device, or transmitted through communications media from one application to another. To support the interchange of SPDL documents in a variety of environments, SPDL provides two document representation formats: a binary interchange format and a clear text interchange format.

This standard is intended to be used for documents that are generated by any text processing system. It is particularly applicable to:

- documents that are intended for electronic printed output;
- documents viewed on windowing systems; and
- documents that are interchanged among systems with differing text output devices.

Level of consensus: This document is scheduled to become an international standard by mid-1993.

Product availability: There are no implementations of SPDL. There are, however, many implementations of the original specification that was modified to become the proposed international standard.

Completeness: The current specification is able to completely describe the page layout of virtually any document or image type for display, print, and interchange requirements in either binary or clear text representations.

Maturity: The specification is based on several existing page description language products (e.g., PostScript) available from different vendors.

Stability: Consensus has evolved on the current specification. No major changes are expected in the next 1 to 3 years.

De facto usage: If users do not reference this specification in procurements, vendors will propose products that do not meet this specification, or that are not compatible with this specification.

Known problems/limitations: None.

Conformance testing: NIST is developing an SPDL interpreter for implementing a conformance testing program.

Future plans: This specification is the basis for a proposed FIPS for SPDL. The FIPS is expected to be adopted by mid-1993, or as soon thereafter as the international standard is adopted.

Alternative specifications: None.

4.11.4 Manuscript Markup Interchange

Specification title: Electronic Manuscript Preparation and Markup (EMPM) ANSI/NISO Z39.59-1988

Specification available from: ANSI, AAP

Publication date: 1988

Sponsoring organization: ISO/IEC JTC1

Applicability: Electronic Manuscript Preparation and Markup is a specialized Document Type Definition (DTD) that includes an architecture encoded in SGML (see sec. 4.11.2) suitable for the interchange of the logical structure of books, articles, and serials. It provides a high-level language for describing these logical structures.

Level of consensus: EMPM is a national standard initially developed by the Association of American Publishers (AAP) and available as ANSI/NISO Z39.59-1988.

Product availability: Implementations are available generally within products that also implement SGML document interchange, such as SGML editors and conversion utilities.

Completeness: The standard offers a complete set of markup for logical structure of specific document types. The standard offers little assistance with layout and presentation style issues.

Maturity: The logical structure of documents is well known and captured in such documents as the Chicago Manual of Style.

Stability: The position as standard for the markup of logical structure makes this a very stable standard. No changes are expected within the next 2 years.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: The physical appearance of documents is not covered.

Conformance testing: None is specified directly for EMPM. The base standard for the formulation of EMPM, SGML, does, however, specify conformance testing.

Future plans: None.

Alternative specifications: Open Document Architecture (ODA) standard ISO 8613:1989, is an alternative international standard for representing the logical structure of documents. Several organizations have designed alternative nonproprietary architectures with SGML encodings. Those organizations are the Association of American Publishers (AAP), the

Text Encoding Initiative (TEI), and the Department of Defense CALS program. Many vendors still recommend that organizations require unique nonstandard document architectures encoded in SGML.

4.11.5 Graphics Data Interchange

Specification title: Computer Graphics Metafile (CGM), FIPS PUB 128

Specification available from: NTIS

Publication date: Revision expected to be approved by mid-1993.

Sponsoring organization: Standards Committee X3H3

Applicability: Graphics data interchange is specified in terms of a file format that can be created independently of device requirements and translated into the formats needed by specific output devices, graphics systems, and computer systems. The standard specifies the content of graphic data interchange.

Level of consensus: The FIPS is based on national and international standard ANSI/ISO 8632:1992 for neutral (implementation and machine independent) graphics file formats. Vendors commonly use CGM as an exchange format for the storage, interchange, or output of a wide range of graphical pictures (from slides for presentation graphics or business charts to diagrams generated by scientific applications). Most CGM implementations conform to the CALS Application Profile (CALS AP), which is the DoD effort to standardize technical documents and engineering drawings. The FIPS recommends the use of the CALS application profile.

Product availability: Numerous CGM implementations exist for use in Federal procurements. Virtually all major microcomputer software products that utilize graphics can generate or interpret CGM files.

Completeness: CGM contains capabilities to describe and format virtually any type of picture or drawing. It has a global symbol capability, the capability for three-dimensional geometry, and engineering drawing capabilities such as control over fine details of line drawings.

Maturity: CGM research and development has been performed for the past 10 years.

Stability: The CGM standard has been revised to include additional graphics functionality and to correct defects in the standard. The standard defines three versions of the Computer Graphics Metafile. Version 1 metafiles are as defined by the original CGM standard document (ISO 8632:1987). Version 2 and Version 3 metafiles are as defined by the amendments to the CGM standard.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are

compatible with it. Users should be careful to specify any subsetting of the CGM capabilities that are allowed and should note that the FIPS does not specify what is allowable as subset implementations.

Known problems/limitations: If an image is not completely specified in the CGM file (e.g., whether or not text fonts are solid or outline) an application may invoke default values for interpreting the image.

Conformance testing: NIST is currently operating a CGM test service to test for conformance of both CGM metafiles and CGM generators. The Metafile Test Service tests binary encoded metafiles for conformance to FIPS PUB 128 or the CALS Application Profile (AP) as defined in MIL-D-28003, "Military Specification: Digital Representation for Communication of Illustration Data: CGM Application Profile." A certificate of validation will be issued for metafiles passing the tests with no failures. The Generator Test Service tests CGM generators (i.e., software that produces CGM metafiles) for conformance to both FIPS PUB 128 and the CALS AP. A certificate of validation will be issued only for implementations that pass *both* sets of tests with no failures. A registered report will be issued after the tests are conducted. If test failures have occurred, the specific failures will be noted in the registered report.

Future plans: Work is in progress on an amendment to the CGM standard, "Rules for Profiles," which will provide rules for defining valid profiles or subsets of ISO/IEC 8632:1987.

Alternative specifications: None.

4.11.6 Graphical Product Data Interchange

Specification title: FIPS PUB 177 Initial Graphics Exchange Specification (IGES)

Specification available from: NTIS

Publication date: December 1992

Sponsoring organization: IGES/PDES

Applicability: IGES standardizes the representation of specific types of complex graphic objects and attributes for data interchange. In this instance, product data interchange encompasses technical drawings, documentation, and other data required for product design and manufacturing, including geometric and nongeometric data such as form features, tolerances, material properties, and surfaces. The information typically associated with computer-aided design and manufacturing (CAD/CAM) can be described. IGES does not cover the complete lifecycle of manufactured products: it addresses only the specification of products; not the manufacturing process relationships.

Level of consensus: The specification was originally defined in National Bureau of Standards Interim Report (NBSIR) 88-3813. It has been defined as ANSI standard, ANSI

Y14.26-1989 (also known as IGES 4.0), by the American Society of Mechanical Engineers (ASME).

Product availability: Numerous implementations of IGES are available in the marketplace.

Completeness: IGES defines the representation of engineering data, but does not include all interfaces for use, such as the interface between the data specification and numerically controlled machining tools.

Maturity: The processes of machine numerical control have been defined and enhanced in direct relation to the requirements for defining and using exchange specifications for engineering data.

Stability: No substantial changes are foreseen in the near term. As the specification advances with newer versions, compatibility will be maintained.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: Not all interfaces between the data exchange specification and external components, such as human/computer interface and machine interfaces have been defined.

Conformance testing: Testing is performed by CAD/CAM Data Exchange Technical Centre (CADETC), UK.

Future plans: IGES Version 5.1 has been released for comment and review. IGES Version 6.0 will be processed as an ANSI standard.

Alternative specifications: STEP (See sec. 4.11.7).

4.11.7 Product Lifecycle Data Interchange

Specification title: Standard for the Exchange of Product Model Data (STEP) Draft Proposed ISO 10303

Specification available from: ISO TC184/SC4 Secretariat (NIST)

Publication date: Draft available.

Sponsoring organization: ISO

Applicability: STEP is an advanced form of representing complex data objects for interchange. It is used in total lifecycle descriptions of engineered products that can be implemented on advanced manufacturing systems. This includes specification of products throughout the stages of their lifetimes. These stages consist of initial concept design,

engineering analysis, manufacturing production, and product support. ISO 10303 consists of multiple volumes. These volumes specify the elements of the STEP strategy (i.e., Application Protocols, Information Models, Implementation Methods, Conformance Tools, and Description Methods).

Level of consensus: The specification is defined in ISO committee draft International Standard 10303. (STEP was previously known as Product Data Exchange Specification [PDES], but the name of the proposed standard was changed to differentiate it from PDES which is actually the initiative that is creating STEP. PDES is now called Product Data Exchange using STEP.)

Product availability: Vendors are engaged in development of prototype implementations of small subsets of the specification.

Completeness: The standard defines a complete product lifecycle including all aspects of describing technical diagrams and documents in a neutral format for transmission over communications networks and processing by numerically controlled machining and assembly tools.

Maturity: STEP was initially built on the concepts of IGES and was extended to include the full lifecycle of products from initial requirements and design through final production and installation.

Stability: STEP is still in a committee draft stage and may undergo revision at any time. Many of the component specifications have not been defined. The initial release of STEP as an international standard is expected in 1994.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: Many of the component specifications have not yet been defined.

Conformance testing: None.

Future plans: STEP will be proposed as an international standard when full agreement has been reached. This is expected in 1994.

Alternative specifications: IGES

4.11.8 Electronic Data Interchange

Specification title: FIPS PUB 161 Electronic Data Interchange (EDI)

Specification available from: NTIS

Publication data: March 29, 1991

Sponsoring organization: X12, United Nations Working Party UN/ECE/WP.4

Applicability: Electronic data interchange (EDI) is a procedure in which instances of documents to be interchanged between separate organizations are converted to strictly formatted sequences of data elements and transmitted as messages between computers. The strict formatting permits computer programs to assemble and disassemble the messages and communicate the data of the messages to and from application programs. EDI is intended primarily for documents that are nontext (i.e., that consist of a sequence of numeric or alphanumeric fields), although an application standard has been developed that allows for the inclusion of product specifications in the form of graphics as parts of such messages. Typical applications are in the procurement process, such as transmitting invoices and purchase orders, and for governmental regulatory activities, such as submission of tax returns and customs forms.

Implementation of EDI requires a family of standards. A family must include (1) syntax standards that specify message organization, the character set for data, and the control characters that start, end, and separate data elements and other groupings within the message; (2) standards for message envelopes that enable a communications protocol to carry and direct the message; (3) data element standards that specify data element types, and for some data elements, the list of data items permitted; (4) data segment standards that form meaningful groupings of data elements; and (5) standards for specific document types.

Level of consensus: There are two widely used families of standards. The U.S. domestic standards have been developed by ANSI-accredited standards committee, X12. There may be as many as 30,000 domestic implementations of X12 EDI at this time. The international family of standards, called EDIFACT (EDI For Administration, Commerce, and Transport) is developed and maintained by the United Nations Economic Commission for Europe, Working Party Four on Trade Facilitation (UN/ECE/WP.4). U.S. input to EDIFACT development is through the Pan American EDIFACT Board, one of five EDIFACT boards that cover the world. There may be several thousand EDIFACT implementations at this time, and the X12 committee has recently voted to adopt the EDIFACT syntax by 1997.

Product availability: Implementation software is widely available. Users with more than a few interchange partners employ computer-based networks as store-and-forward delivery agents. These so-called value-added networks, or VANs, are similarly widely available.

Completeness: The two families of standards, X12 and EDIFACT, are complete to the extent that the syntax and supporting standards are available to enable interchanges to occur for any document type that has been standardized. Development of standards that support additional document types is continuing at a rapid pace in both families of standards.

Maturity: The concept is proven, and the number of implementations continues to increase.

Stability: New versions and releases are being produced approximately on a yearly basis. Users need to stay current. The conversion of X12 implementations to EDIFACT could introduce costs of retrofitting.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: The acceptance of electronic documents in a court of law has been considered questionable in the past. With wide use of EDI, and with change and/or reinterpretation of statutes and regulations, as well as with adoption of electronic techniques for originator authentication and transmission integrity, this issue will be less important in the future. Maintenance of audit trails and assurance of trustworthy record-keeping will assist, however, in providing confidence in the authenticity of electronic documents.

Conformance testing: NIST is studying this issue at the present time.

Future plans: FIPS PUB 161 will be updated to reflect X12 adoption of EDIFACT standards. The implementation of a Federal digital signature standard and development of a national infrastructure for management and distribution of cryptographic keys for that standard will promote the use and acceptance of EDI. Development of products that implement CCITT standards X.400, X.435, and the X.500 series will further enhance EDI as an accepted data interchange procedure.

Alternative specifications: None.

4.11.9 Spatial Data Interchange

Specification title: FIPS PUB 173 Spatial Data Transfer Standard (SDTS)

Specification available from: National Mapping Division, U.S. Geological Survey (USGS)

Publication date: Draft available.

Sponsoring organization: USGS

Applicability: This standard is mandatory in the acquisition and development of government applications and programs involving the transfer of digital spatial data among heterogeneous computer systems. The use of the SDTS applies when the transfer of digital spatial data occurs, or is likely to occur, within or outside of the Federal government. SDTS is not tied to particular data structures, classes of computer platforms, or distribution media.

Level of consensus: A recent Geographic Information System (GIS) industry survey indicates that 65 percent of GIS vendors intend to support SDTS. This is significant since more than 90 percent of GIS are turn-key systems. Many of the specifications included in SDTS have long histories of development and use.

Product availability: The U.S. Geological Survey (USGS) has developed public domain software for encoding and decoding data into and out of the SDTS neutral exchange file.

Completeness: SDTS provides specifications for the organization and structure of digital spatial data transfer, definition of spatial features and attributes, and data transfer encoding.

Maturity: Work began on this standard in 1982 with the participation of academia, industry, and the U.S. Government. International efforts to develop a spatial data interchange standard have all emulated SDTS in various ways. The testing, modification, and refinement of SDTS has occurred over an 8 year period.

Stability: SDTS was designed to be modular and extensible. The neutral exchange format specified for SDTS implementation is independent of SDTS.

De facto usage: GIS technology is fundamental to all governmental organizations, and vendors will likely propose products that will meet the SDTS specification or are compatible with it.

Problems/limitations: Unknown

Conformance Testing: Software for conformance testing of SDTS is currently being planned.

Future plans: The SDTS Vector Profile has undergone several revisions and is now in the final refinement and testing phase. SDTS Raster Profile development is underway.

Alternate specification: None

4.12 Graphics Services

Graphics services provide the interfaces for manipulating and programming applications concerning images and graphics in a device-independent manner. The specifications included in this service area are the Graphical Kernel System (GKS) FIPS PUB 120-1, and the Programmer's Hierarchical Interactive Graphics System (PHIGS) FIPS PUB 153. They are targeted at different types of users and applications.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
FIPS PUB 120-1 GKS	●	●	●	●	●	●	●
FIPS PUB 153 PHIGS	●	●	●	○	●	●	●

Legend: ●-high evaluation ○-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.12.1 Two-Dimensional Graphics API

Specification title: FIPS PUB 120-1 Graphical Kernel System (GKS)

Specification available from: NTIS

Publication date: January 8, 1991

Sponsoring organization: Standards Committee X3H3

Applicability: This specification fulfills the requirement for a language to program two-dimensional graphical objects that will be displayed or plotted on appropriate devices (raster graphics and vector graphics devices).

Level of consensus: The GKS FIPS is based on ANSI Standard X3.124-1985 and ISO Standard 7942:1985. Bindings for Ada, Fortran, and Pascal have been defined and standardized.

Product availability: A full range of products and automated tools based on GKS has been available from various vendors for 5 or more years.

Completeness: The standard includes constructs and library calls for virtually any kind of two-dimensional graphic image.

Maturity: Initial work started on this specification in 1978 and has been developed substantially by international organizations in the ensuing years. It was founded on a graphics standards methodology developed in 1976.

Stability: No changes are foreseen.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: None.

Conformance testing: NIST has licensed a conformance test suite for GKS. Using this test suite, NIST is currently operating a GKS Test Service to test implementations for conformance to the FIPS. The test suite is available for the Fortran binding to GKS. A registered test report will be issued after the conduct of tests. A certificate of validation will be issued only to implementations passing the tests with no failures. If failures have occurred, the specific failures will be identified in the registered test report. The results of tests on individual implementations that have passed will be posted in the Validated Products List (VPL) which is published quarterly by NIST.

Future plans: The GKS test suite will undergo revision as warranted.

Alternative specifications: PHIGS (see sec. 4.12.2)

4.12.2 Interactive and Three-dimensional Graphics API

Specification title: FIPS PUB 153 Programmer's Hierarchical Interactive Graphics System (PHIGS)

Specification available from: NTIS

Publication date: October 14, 1988

Sponsoring organization: Standards Committee X3H3

Applicability: This specification fulfills the requirement for a language to program two- and three-dimensional graphical objects that will be displayed or plotted on appropriate devices in interactive, high-performance environments, and for managing hierarchical database structures containing graphics data.

Level of consensus: The FIPS is based on ANSI Standards X3.144-1988 and X3.144.1-1988, and ISO Standard 9592:1988.

Product availability: Numerous implementations are available for various hardware/software platforms.

Completeness: PHIGS is a full-functioned specification for the development of interactive two- and three-dimensional graphics applications that manage hierarchical database structures containing graphics data. Bindings for Fortran, C, and Ada have been adopted.

Maturity: Many of the concepts for this standard were drawn from previous work. Chief among those works are the Association for Computing Machinery (ACM) SIGGRAPH Graphics Planning Committee Core Graphics System and the Standard Graphical Kernel System (GKS) ANSI X3.124-1985.

Stability: No changes are planned in the next 1 to 3 years.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it.

Known problems/limitations: Unknown

Conformance testing: Version 2.0 of the NIST PHIGS test suite and a formal PHIGS test service became available from NIST on October 1, 1992. The PHIGS test suite tests implementations using the Fortran binding for conformance to the FIPS. A registered test report is issued upon completion of testing. A certificate of validation will be issued only to implementations passing the tests with no failures. If any failures have occurred, they will be identified in the registered test report. A C binding version of the test suite will be available in late 1993.

Future plans: A binding for Pascal is under development. A new standard, called PHIGS Plus, is being developed which adds shading, lighting, and other advanced graphics programming capabilities that were not intended for inclusion in the original version. Conforming PHIGS programs will be able to execute under PHIGS Plus with no changes.

Alternative specifications: None.

4.13 Network Services

This area of the APP includes data communications, transparent file access, personal/microcomputer support, distributed computing support, distributed systems management, and network application program interfaces.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	DFU	PRL
PII API IEEE P1003.12		O		O		●	
ACSE IEEE P1238							
FTAM IEEE P1238.1		O			O		
FIPS PUB 146-1 GOSIP 2	●	●	●	●	●	O	O
ISDN ASI	●		O	●	O	O	O
ISDN	O		O	O	O	O	●
DCE RPC					O		
TFA IEEE P1003.8		O	●	●			
FIPS PUB 179 GNMP	●		O	●	●		O
X.400 API IEEE P1224.1	O		●	O	●	O	●
X.500 API IEEE P1224.2	O		●	●	●	●	●

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

4.13.1 Communication API for Protocol Independent Interfaces

Specification title: Protocol Independent Interfaces (PII) IEEE P1003.12 Draft 2.0

Specification available from: IEEE

Publication date: Draft available

Sponsoring organization: IEEE

Applicability: P1003.12 defines the protocol-independent application interfaces to enable one process to communicate with another local process or a remote process over a network. Draft Version 2.0 will consist of a low-level interface specification.

The Detailed Network Interface (DNI) specification supports protocol-independent local and network process-to-process communications with access to protocol-dependent

features. DNI is intended to provide access to protocol-specific features of the underlying network for highly portable applications that need access to sophisticated network features. Since two currently recognized industry practices in the DNI specification are X/Open Transport Interface (XTI) and BSD Socket interface, a dual DNI standard (DNI/XTI and DNI/sockets) specification is being created for P1003.12. The DNI/XTI and DNI/Sockets APIs will provide transport layer access. The DNI/Socket API will also allow access to lower OSI layers. The intermixing of DNI/XTI calls and DNI/Sockets will not be specified. That is, the specification will not prescribe what combinations or subsets of both XTI and Sockets should be implemented.

Level of consensus: The first ballot is expected soon after the July 1993 POSIX meetings.

Product availability: Products currently exist based on XTI and sockets.

Completeness: The completed specification will contain language independent specification (LIS) and C bindings in addition to Test Methods.

Maturity: The draft specification incorporates the technology of the XPG4 version of the X/Open CAE Specification—X/Open Transport Interface (XTI), dated January 1992, and the 4.4 BSD sockets interface, with interface mappings to ISO Transport and Internet Transport information for XTI. These are implementations of products that have existed for 5 or more years.

Stability: The specification requires significant effort in the areas of LIS specification, LIS test assertions generation, sockets semantics documentation, sockets test assertions generation, and verification of consistency with other POSIX standards. While all sections of the document may be affected by the consistency verification, the bulk of the changes will relate to the LIS and sockets. The LIS is in a definition phase. The sockets activity is largely one of documenting the current semantics.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will probably propose products that meet this specification or are compatible with the specification.

Known problems/limitations: Certain areas of the specification require liaison with other groups including P1003.1, P1003.4, P1003.6, and P1003.17. For Draft 2.0, the Simple Network Interface (SNI) and the Naming Interface are not included. Work on these areas has been postponed in order to process a ballot of the DNI specification in mid-1993.

Conformance testing: Test methods will be defined for measuring the conformance of implementations to this specification. Work on XTI assertions is under way.

Future plans: Considerable work still needs to be done on the Simple Network Interface (SNI) and the Naming Interface. SNI and the Naming Interface will be included in the future.

Simple Network Interface (SNI) will support protocol-independent network process-to-process communications in a protocol-independent manner. SNI is intended to provide a simple view of underlying networks for portable applications that do not need access to sophisticated network features.

The Naming Interface will support naming/addressing needs for SNI and DNI. The P1003.12 naming interface will be based on the P1224.2 naming interface and P1224 Object Management work.

Alternative specifications: X/Open CAE Specification—X/Open Transport Interface (XTI), January 1992.

4.13.2 Communication API for OSI Services

Specification title: OSI ACSE/Presentation Application Program Interfaces IEEE P1238

Specification available from: IEEE

Publication date: The expected publication date for the completed specification is early 1994.

Sponsoring organization: IEEE

Applicability: This specification provides an API between applications and the OSI Association Control Service Element (ACSE) and presentation services.

Level of consensus: Consensus has not been reached on a base document for an OSI ACSE/Presentation API.

Product availability: Products conforming to P1238 are not expected until late 1994.

Completeness: The specification will have language-independent and C language bindings, as well as Test Methods.

Maturity: The specification is under development. The underlying model is the OSI seven-layer model which enjoys a large following.

Stability: Numerous changes in the specification can be expected over the next 1 to 2 years.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification. The P1238 specification is being used primarily by the FTAM API which is under development by the same working group.

Known problems/limitations: Suitability of different language bindings may be a concern, as well as high-level to low-level mappings among different layers in the OSI Reference Model.

Conformance testing: Test assertions are under development as part of the specification. These assertions are compatible with existing ACSE/Presentation tests.

Future plans: The Industry/Government Open Systems Specification (IGOSS) will reference this specification when it is completed. Until then, adherence to this developing specification is suggested. Final approval of the P1238 specification is scheduled for early 1994.

Alternative specification: None

4.13.3 File Transfer API

Specification title: OSI API for File Transfer, Access, and Management (FTAM) IEEE P1238.1

Specification available from: IEEE

Publication date: The expected publication date for a completed specification is mid-1994.

Sponsoring organization: IEEE

Applicability: This specification is designed for use as a standard application interface to File Transfer, Access, and Management (FTAM) implementations. These are the APIs for locating files, controlling low-level connections between file systems, and accessing the files.

Level of consensus: This specification defines an API for the protocols defined in ISO 8571, Parts 1-5, and the OIW Implementation Agreements, NIST Special Publication 500-202, "Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 5, Edition 1," December 1991, and Draft "Working Implementation Agreements for Open Systems Interconnection Protocols." No consensus has been reached on a base specification for this API.

Product availability: De facto FTAM API products are available. Products conforming to the P1238.1 specification are not expected until late 1994.

Completeness: The specification will have language-independent and C language bindings, as well as Test Methods.

Maturity: The FTAM concept has existed in various forms over the last 7 years. The codification process has been underway for over 2 years.

Stability: The FTAM standard and corresponding OIW Implementation Agreements are both very stable. The specification has stabilized to a level of minor adjustments to correct inconsistencies.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: The specification does not differentiate between high- and low-level file operations.

Conformance testing: Test assertions are under development as part of the specification. These test assertions will be used to develop specific validation and interoperation test cases.

Future plans: Final approval is scheduled for early 1994. Future versions of IGOSS are expected to reference the approved draft.

Alternative specification: None.

4.13.4 Communication Protocols for OSI

Specification title: FIPS PUB 146-1 Government Open System Interconnection Profile (Version 2.0)

Specification available from: NTIS

Publication date: April 1991

Sponsoring organization: OSE Implementor's Workshop

Applicability: GOSIP is mandatory for all data communications environments where interoperability is desired. GOSIP is based on Open Systems Interconnection (OSI) standards, the world-wide consensus standards for multivendor data communications based on OSI protocols. The GOSIP protocols provide interoperability among applications in a heterogeneous network.

GOSIP mandates no service interface accessibility. Therefore, any service interface accessibility requirements must be clearly stated and mandated in procurement documentation. For example, GOSIP mandates no specific direct access to transport services. If the acquiring authority requires direct access to transport services, such a requirement must be included in a solicitation. The issues involved in determining such a requirement are complex. Refer to the "Government Open System Interconnection Profile (GOSIP) Users' Guide," NIST Special Publication 500-192, for a discussion of these issues.

Level of consensus: The GOSIP FIPS is based on the ISO and CCITT international standards, implementors agreements developed at the OSE Implementor's Workshop, and

U. S. Government requirements. (The OSE Implementor's Agreements are specified in NIST Special Publication 500-202, "Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 5, Edition 1," December 1991, and Draft "Working Implementation Agreements for Open Systems Interconnection Protocols.") DoD has mandated GOSIP use in all computer communications procurements for all services. In addition, the Departments of Energy and Veterans Affairs, as well as other Federal agencies, have specified the use of GOSIP in procurements.

Product availability: Various products implementing specific protocol levels of the OSI layered model have been produced and conform to the FIPS. Vendors are given an 18-month period between promulgation of a new version of GOSIP and the date that it must be referenced in Federal procurements to ensure that new products will be available.

Completeness: GOSIP is essentially a family of protocols and representation specifications. It provides a complete transparent, end-to-end data communications capability based on OSI transport class 4 (TP4) and connectionless network protocol (CLNP). GOSIP Version 1.0 provides electronic mail and file transfer access and management applications. It operates over a variety of local and wide area network technologies. Version 2.0 adds remote logon and office document interchange applications, a new network addressing structure to support dynamic routing, provision to operate over an Integrated Services Digital Network (ISDN), and allows an optional connectionless transport service to support transparent file access (see sec. 4.13.8) and other applications.

Maturity: As of October 3, 1992, GOSIP Version 2.0 became a mandatory requirement in Federal information processing (FIP) resources procurements. GOSIP Version 3.0, which will reference the services and protocols contained in the IGOSS, is expected to be mandated for Federal procurements initiated in late 1995.

Stability: The GOSIP process is extremely stable. New versions of existing protocols will be upwardly compatible with current versions.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it. (Notwithstanding the fact that TCP/IP is widely used in Government communications, especially DoD networks, GOSIP is mandated for all Federal communications procurements and major communications upgrades after October 1992.)

Known problems/limitations: Known problems/limitations include testing, transition, international harmonization, and the need for additional functionality.

Conformance testing: The U.S. GOSIP Testing Program permits Federal Agencies to substantiate claims of GOSIP compliance through conformance and interoperability testing. The U.S. GOSIP Register Database (GORD) contains up-to-date reference information. Lists of GOSIP-conformant products are published in the quarterly Validated Products List (VPL).

Future plans: A future version of GOSIP will include added functionality. Key features may vary with specific combinations of vendor products and users. NIST is producing guidelines for users to evaluate which applications are best for individual requirements. The Industry/Government Open Systems Specification (IGOSS), upon which GOSIP Version 3.0 will be based, represents a collaboration between the Manufacturing Automation Protocol/Technical and Office Protocols (MAP/TOP) Working Group, the Electric Power Research Institute (EPRI), the Canadian Government, and the U.S. Government. It is expected to be promulgated in 1993. Additional functionality expected includes the following: (1) Message Handling Systems (MHS) Extensions; (2) Electronic Data Interchange (EDI) User Agent; (3) File Transfer, Access and Management (FTAM) Extensions; (4) Directory Services; (5) Remote Database Access; (6) Distributed Transaction Processing; (7) Manufacturing Message Specification; (8) X-Windows over OSI; (9) Information Retrieval; (10) Fiber Distributed Data Interface (FDDI); (11) Frame Relay; (12) Intermediate System-Intermediate System (IS-IS) routing and Inter-Domain Routing Protocol (IDRP); (13) Network Management; and (14) Connectionless Upper Layer Service. OSI standards have been developed over the last 10 years and are based on a well-understood reference model, the Open Systems Interconnection (OSI) seven-layer communications model.

Alternative specifications: None.

4.13.5 Communication API for Integrated Digital, Video, and Voice

Specification title: Application Software Interface (ASI) Version 1 (for accessing and administering Integrated Services Digital Network [ISDN] services)

Specification available from: NIST

Publication date: June 5, 1992

Sponsoring organization: NIST

Applicability: The Application Software Interface (ASI) focuses on the definition of a common application interface for accessing and administering ISDN services provided by hardware commonly referred to in the vendor community as Network Adapters (NAs).

Level of consensus: The ASI is based on the implementation agreements produced by the North American ISDN Users' Forum (NIUF). These agreements are, in general, based upon relevant ANSI standards.

Product availability: Current products are proprietary products based on proprietary specifications. Products based on ASI Version 1 are expected to emerge during 1993.

Completeness: The ASI is an evolving specification. Items for inclusion are based on services defined in ANSI and the NIUF. As the definitions emerge from these bodies, they are included in the ASI.

Maturity: While ISDN usage is not widespread, the technology is well defined and understood. The ASI specification provides a uniform interface to these services.

Stability: This specification is an evolving interface and changes are anticipated to incorporate new features. These changes are primarily due to additional ISDN features as specified by ANSI and the NIUF. These changes are expected to be in the form of additions to the existing specification, not a replacement.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: The greatest known problem is the limited set of service definitions available through the ASI today. As the services are defined in the standards bodies and the NIUF, the service definitions will be included in the ASI.

Conformance testing: Conformance tests are planned for the ASI.

Future plans: The ASI will continue to include additional ISDN services in its specification. Additional work includes device control and an additional higher level interface. Future versions of the FIPS for ISDN are expected to include the ASI. The ASI is expected to be submitted for consideration as an ANSI standard.

Alternative specification: None.

4.13.6 Communication Protocols for Integrated Digital, Video, and Voice

Specification title: NIST Planned FIPS on Integrated Services Digital Network (ISDN)

Specification available from: NIST

Publication date: Draft available.

Sponsoring organization: NIST

Applicability: The proposed FIPS PUB compiles the existing NIUF agreements for ISDN as developed and approved in the NIUF as of November 1990. These agreement are published in NIST Special Publication 500-195, dated September 1991. These agreements cover Layer 1 Basic Rate Interface (BRI) at the U, and S/T reference points; Layer 1 Primary Rate Interface (PRI) at the U reference point; Layer 2 BRI and PRI; Layer 3 BRI Basic Call Control for Class I equipment; and Layer 3 PRI Basic Call Control for Class II equipment.

Level of consensus: The proposed ISDN FIPS is currently undergoing comment resolution in the review process. Final approval is expected mid-1993. The proposed ISDN FIPS is

based on the implementation agreements produced by the NIUF. These are, in general, based upon relevant ANSI standards.

Product availability: Currently, only proprietary products are available. Vendors will soon propose products based on Bellcore National ISDN-X (NI-X), for which the current version is NI-1. Plans are for NI-3 to become aligned with the ISDN FIPS during 1995. At that time, NI-3 compliant products will also be compliant with the ISDN FIPS.

Completeness: The ISDN FIPS will adopt the implementation agreements from the NIUF. These agreements evolve through an ongoing process. The ISDN FIPS is based on the agreements as published in NIST Special Publication 500-195, September 1991. As additional agreements are made, these will become a part of future revisions of the FIPS.

Maturity: While ISDN usage is not widespread in the United States, the technology is well defined and understood. Standards for ISDN have existed for a number of years.

Stability: While the specification is a proposed FIPS, few changes are expected during the comment process. It is expected that this FIPS will be revised to include additional implementation agreements from the NIUF.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: None.

Conformance testing: The proposed FIPS references the conformance tests that have been completed by the NIUF. These include the Layer 1 BRI S/T interface and the Layer 2 BRI Link Access Procedures D (LAPD). Plans exist for continuing this process.

Future plans: The Bellcore National ISDN-X process is producing a set of ISDN implementations that should be aligned with the NIUF by NI-3 in the 1995 timeframe. Vendors are now implementing NI-1. The work of the NIUF is an ongoing process. This work will be included in future revisions of the FIPS as updates to implementation agreements.

Alternative specifications: Bellcore National ISDN 1. GOSIP references ISDN; however, the ISDN referenced by GOSIP only contains a small amount of the functionality contained in the proposed FIPS.

4.13.7 Remote Procedure Call

Specification title: OSF Distributed Computing Environment (DCE) Remote Procedure Call (RPC) Component

Specification available from: Open Software Foundation (OSF)

Publication date: Draft available.

Sponsoring organization: OSF

Applicability: Distributed computing services include specifications for remote procedure calls and distributed realtime support in heterogeneous networks (as opposed to single node support as specified in operating system services). Distributed access services include functional support for submitting, starting, and stopping processes among processors in a heterogeneous network. OSF RPC includes support for naming, dynamic binding, and security (authentication, data privacy, and integrity protection). An API for OSF RPC is defined.

Level of consensus: The content of OSF RPC is determined by OSF members.

Product availability: Vendor partial implementations are available and based on the OSF specification.

Completeness: No specifications exist that define a complete set of functions necessary to provide remote procedure communications for all types of application platforms (i.e., the language-independent representation of remote procedure calls). OSF RPC contains a language mapping for C.

Maturity: In general, OSF specifications are based on object-oriented structures and relationships. The underlying services and data formats are well-established, but the objects to be managed are still evolving.

Stability: Other industry consortia are reviewing the possibility of adopting OSF RPC. Other specifications are emerging as possible alternatives.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification, or that are not compatible with the specification.

Known problems/limitations: The specification is incomplete and still in a draft state.

Conformance testing: Validation suites will be available at the time the specification is complete for OSF RPC.

Future plans: Continued development of the specification to include new technology as it becomes available.

Alternative specifications: ONC RPC (Open Network Computing Remote Procedure Call). When the ISO 11578 RPC standard is complete, it will supersede other RPC specifications. At this point, it still needs significant work to complete.

4.13.8 Transparent Network Access to Remote Files

Specification title: Transparent File Access (TFA) IEEE P1003.8 Draft 7

Specification available from: IEEE

Publication date: Draft available.

Sponsoring organization: IEEE

Applicability: Transparent file access includes capabilities for managing files and transmitting data through heterogeneous networks in a manner that is transparent (i.e., does not require knowledge of file location or of certain access requirements) to the user. In a GOSIP environment, TFA should be based on the services provided by FTAM.

Level of consensus: This specification is still in a draft stage. The first ballot was completed in May 1992. The specification entered first recirculation ballot in early 1993 (i.e., ballot on resolution of actions stemming from first ballot).

Product availability: Many functions of TFA are widely available in existing vendor implementations of network oriented file systems and have interfaces that closely resemble the TFA interface. (These implementations may or may not be based on FTAM services.)

Completeness: The specification is in draft form but is essentially complete. It is still subject to modification during the balloting process.

Maturity: Much research on distributed file access and file systems has been performed and published over the last 10 years. As a consequence, many of the problems of distributed files and file systems have become known and various solutions have been developed. There are still areas of distributed file access, such as global address resolution, concurrency, and security that will have profound effects on TFA functionality. In some cases, the capabilities of hardware and software that are available today cannot support the requirements of TFA in all cases. A minimal set of functionality has been identified.

Stability: Significant changes in the specification are unlikely, but numerous smaller changes are anticipated. This could have a cascading effect on other parts of the specification. Until consensus on the minor aspects of major features is reached, one must consider the specification in a state of flux.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: Currently, there is no specification for the file system semantics that result from most implementations of systems with TFA-like features. Such systems are usually referred to by the protocols that each implementation uses (e.g., NFS, RFS, AFS, NCS). The eventual TFA specification should overcome this limitation.

Conformance testing: None.

Future plans: A specification is expected to be proposed as a FIPS by late 1993.

Alternative specifications: None.

4.13.9 Network Management

Specification title: FIPS PUB 179 Government Network Management Profile (GNMP) Version 1.0

Specification available from: NTIS

Publication date: December 14, 1992

Sponsoring organization: NIST

Applicability: The GNMP is the standard reference for all Federal Government agencies to use when acquiring Network Management (NM) functions and services for computer and communication systems and networks.

Level of consensus: This specification has been aligned with an industry published specification, the Open Management Roadmap OMNI*Point* 1 specification. The OMNI*Point* 1 specification represents the results of the Open Management Roadmap activity. The Open Management Roadmap activity is a partnership of government, industry, vendors, and users, initiated and managed by the Network Management Forum (NMF) to coordinate all related network management activities of developing standards and defining specifications to produce interoperable network management products. Currently, the partnership includes: Her Majesty's Treasury, U.K. (CCTA), European Community Testing Services for Network Management (CTS3/NM), the National Institute of Standards and Technology (NIST), the Network Management Forum (NMF), X/Open, the Object Management Group (OMG), the Open Software Foundation (OSF), the Corporation for Open Systems (COS), the Interoperability Technology Association for Information Processing (INTAP), the Standards Promotion and Application Group (SPAG), UNIX International (UI), and the User Advisory Council (UAC). Standards organizations and regional workshops, such as the OIW, are source organizations in the Roadmap activity. The Roadmap defines a number of Open Management Network Interoperability Points (OMNI*Points*) that are snapshots of standards, specifications, and agreements for network management to which the vendor partners agree to develop products and for which the user partners expect to purchase products.

Product availability: A few products implement parts and subsets of the specification, but full implementations will probably be available in 1993.

Completeness: For the definition of management information, Version 1.0 GNMP focuses primarily on identifying the information required for managing implementations that incorporate the functionality specified for layers 1 and 2 of the OSI Reference Model.

The second version of the GNMP, planned to be released approximately 18 months after Version 1.0 GNMP is promulgated, will add the information required mainly for managing implementations of the functions specified for layers 3 through 7 of the OSI reference model. Version 3 will specify the management information (MI) required for the management of computer applications and services that are outside of the seven-layer communications stack, such as computer operating systems and database management systems.

Maturity: The primary source of specifications in the Version 1.0 GNMP is part 18 of the "Stable Implementation Agreements for Open Systems Interconnection Protocols," June 1992. This source provides implementation specifications for network management based on the services and protocol standards issued by the ISO/IEC. Version 1.0 GNMP is an integral part of OMNI*Point* 1. The first OMNI*Point* specification, OMNI*Point* 1, was released in August 1992.

Stability: GNMP will undergo revision over the next 3 to 5 years to include new functionality. These additional functions will be backward-compatible with existing implementations.

De facto usage: If users do not reference this specification in procurement documents, vendors will probably propose products that do not meet this specification or that are not compatible with the specification.

Known problems/limitations: The most pressing problem known is that of a lack of a complete set of system object definitions, and security standards for network management.

Conformance testing: NIST plans to provide certification procedures and tests for demonstrating product conformance.

Future plans: Version 2 GNMP is planned to be released approximately 18 months after Version 1.0.

Alternative specifications: OMNI*Point* 1 specification.

4.13.10 Electronic Messaging API

Specification title: X.400 Based Electronic Messaging Application Program Interface (API) IEEE P1224.1 Draft 3

Specification available from: IEEE Working Group P1224.1

Publication date: Draft available.

Sponsoring organization: IEEE

Applicability: X.400 provides electronic mail interoperability among heterogeneous computer systems. X.400 is an international standard protocol definition. The X.400 API

defines an interface between the user of a mail system and the mail system. IEEE P1224.1 is a language-independent specification.

Level of consensus: An IEEE standard is expected in mid-1993. The U.S. Technical Advisory Group (TAG) to ISO/IEC Joint Technical Committee 1 (JTC1) has recommended the X.400 API standard for FASTTRACK (accelerated) approval. It is anticipated that an ISO standard will follow by the end of 1993.

Product availability: Once the standard is complete, numerous products are expected.

Completeness: This specification is a complete detailed level X.400 interface. A high-level interface has not yet been defined. The X.400 API is contained in four documents which are (1) P1224.1—Language Independent Specification; (2) P1326.1—Language Independent Test Methods; (3) P1327.1—C Language Bindings; (4) P1328.1—C Language Test Methods.

Maturity: The principal elements of the X.400 API have been agreed upon for the last 3 years. In time, as the API is fully implemented, the standard will reach a high level of maturity.

Stability: This specification is stable. Tuning modifications can be expected until the final specification is accepted as an IEEE standard.

De facto usage: If users do not reference this specification in procurement documents, it is uncertain whether vendors will propose products that meet this specification or that are compatible with the specification. Procurement documents may have to require this API before it will be widely used in X.400 implementations.

Known problems/limitations: None.

Conformance testing: Test methods have been defined for measuring the conformance of implementations to this specification.

Future plans: The Electronic Data Interchange (EDI) and X.400 Message Store APIs will be addenda to the X.400 API standard. Additionally, a high-level API may be standardized in the future.

Alternative specification: None.

4.13.11 Directory Services API

Specification title: Directory Services Application Program Interface (API) IEEE P1224.2 Draft 5

Specification available from: IEEE Working Group P1224.2

Publication date: November 1992.

Sponsoring organization: IEEE

Applicability: CCITT X.500, which is an international standard protocol definition, provides Directory Services interoperability among heterogeneous computer systems. The Directory Services Application Program Interface (DS API) defines a standard directory service user agent interface to support application portability at the source-code level. Although the DS API is intended to provide access to CCITT X.500 functionality, its scope is not limited to just X.500, and could be used to access other directory services as well. IEEE P1224.2 is a language-independent specification.

Level of consensus: This specification is still in draft stage and has completed a second ballot by IEEE working group members. Final adoption is expected in early 1993. The U.S. TAG to JTC1 has recommended the DS API standard for FASTTRACK approval.

Product availability: Once the standard is complete, numerous products are expected. P1224.2 (and related specifications) are based on X/Open's XDS specification, which has subsequently been adopted by OSF for inclusion in its Distributed Computing Environment (DCE), and by UNIX International (UI) for inclusion in the UI Atlas environment.

Completeness: This specification is a complete detailed level X.500 interface to directory services. The DS API is contained in four documents which are 1) P1224.2 - Language Independent Specification; 2) P1326.2 -Language Independent Test Methods; 3) P1327.2 - C Language Bindings; and 4) P1328.2 - C Language Test Methods.

Maturity: The principal elements of the DS API have been agreed upon for several years. In time, as the API is fully implemented, the standard will reach a high level of maturity. The DS API is based on X/Open's XDS, which is part of the XPG4 specification.

Stability: No significant changes are foreseen over the next 1 to 2 years.

De facto usage: Even if users do not reference this specification in procurement documents, vendors will likely propose products that meet the specification or are compatible with it. This specification is included as an integral part of OSF's Distributed Computing Environment (DCE), X/Open's Common Application Environment, and UI's Atlas.

Known problems/limitations: None.

Conformance testing: Test methods have been defined for measuring the conformance of implementations to this specification.

Future plans: Directory services protocol mapping will be included in future versions of GOSIP.

Alternative specification: X/Open Directory Service (XDS).

5. STRATEGIC EVALUATIONS

As part of the evaluation of APP specifications, users should take into account the strategic value of each specification. Table 2 summarizes NIST's views on the strategic value of each specification recommended in this report.

The valuations are made according to the following guidelines:

a) Strategic now (STR)—In selecting these specifications, users would be reasonably safe in making substantial investment and long-term plans covering mission-critical systems and the infrastructure needed to support them. Changes are expected to be upwardly compatible.

b) Strategic in the future (FTR)—Specifications that are subject to change but appear to be headed for standardization fall into this category. Existing standards that may be subject to changes that are not entirely upwardly compatible also fall into this category. There are some long-term risks involved, but the actions of the consensus-building process will tend to minimize them. Users should select these specifications where strategic specifications are unavailable and an investment must be made, but should plan for possible evolution in the future.

c) Nonstrategic (GAP)—These specifications are stop-gap measures recommended with the warning that any user investment will be at significant risk. They are not appropriate for long-term planning. Users should, for these reasons, minimize their risk by minimizing investment.

Subsequent versions of this report may incorporate this dimension of evaluation in the overall evaluation criteria.

Table 2. Strategic Value of APP Specifications

OSE SERVICE AREA / Applicable Specifications	STR	FTR	GAP
OPERATING SYSTEM SERVICES			
FIPS PUB 151-2 Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]	●		
NIST Planned FIPS PUB on Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities Interface IEEE Std 1003.2-1992, Information Technology—Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities	●		
Amendment 1: Realtime Extension [C Language] IEEE P1003.4		●	
Security Interface for the Portable Operating System Interface for Computer Environments IEEE P1003.6		●	
HUMAN/COMPUTER INTERFACE SERVICES			
NIST Planned FIPS PUB 158-1 for User Interface Component of Applications Portability Profile	●		
Draft Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (IEEE P1295.1)		●	

OSE SERVICE AREA / Applicable Specifications	STR	FTR	GAP
SOFTWARE ENGINEERING SERVICES			
FIPS PUB 119 Ada	●		
FIPS PUB 160 C	●		
FIPS PUB 21-3 COBOL	●		
FIPS PUB 69-1 Fortran	●		
FIPS PUB 109 Pascal	●		
Portable Common Tools Environment (PCTE): Abstract Specification, Standard ECMA-149		●	
DATA MANAGEMENT SERVICES			
FIPS PUB 156 Information Resource Dictionary System (IRDS)	●		
Planned FIPS PUB 127-1 for Database Language SQL	●		
Remote Database Access (RDA)		●	
DATA INTERCHANGE SERVICES			
Office Document Architecture/Office Document Interchange Format (ODA/ODIF) ISO 8613:1989	●		
Standard Page Description Language (SPDL) ISO/IEC DIS 10180		●	
FIPS PUB 152 Standard Generalized Markup Language (SGML)	●		
Electronic Manuscript Preparation and Markup (EMPM) ANSI/NISO Z39.59-1988		●	
FIPS PUB 128 Computer Graphics Metafile (CGM)	●		
FIPS PUB 177 Initial Graphic Exchange Specification (IGES)	●		
Standard for the Exchange of Product Model Data (STEP) Draft Proposed ISO 10303		●	
FIPS PUB 161 Electronic Data Interchange (EDI)	●		
FIPS PUB 173 Spatial Data Transfer Specification (SDTS)	●		
GRAPHICS SERVICES			
FIPS PUB 120-1 Graphical Kernel System (GKS)	●		
FIPS PUB 153 Programmer's Hierarchical Interactive Graphics System (PHIGS)	●		
NETWORK SERVICES			
IEEE P1003.12 Protocol-independent Interfaces		●	
IEEE P1238 OSI ACSE API		●	
IEEE P1238.1 File Transfer Access and Management (FTAM) API		●	
FIPS PUB 146-1 Government Open System Interconnection Profile Version 2	●		
ISDN ASI		●	

OSE SERVICE AREA / Applicable Specifications	STR	FTR	GAP
ISDN Protocols		●	
OSF DCE Remote Procedure Call			●
IEEE P1003.8 Transparent File Access		●	
FIPS PUB 179 Government Network Management Profile (GNMP)	●		
IEEE P1224.1 X.400 Electronic Messaging API		●	
IEEE P1224.2 X.500 Directory Services API		●	

6. CONCLUSION

The long-term goal of the program on which this report is based is the establishment of an open system environment for use in Federal information systems support. In this open system environment, interoperability, portability, and scalability must be the driving forces for the development of standard interfaces, services, protocols, and formats. Eventually, users would like to see all of the OSE specifications take the form of Federal Information Processing Standards (FIPS). In the interim, NIST has reviewed many of the specifications that are now available and has made recommendations on those that are believed to have a higher probability of becoming successful additions to the suite of OSE specifications.

The short term goals of Federal information requirements demand action now. In response to these goals, NIST has developed a suite of specifications that can be used in system development and acquisition. Many of these specifications are Federal standards, and others are national or international standards. These specifications are relatively stable and can be used with little risk.

There is, however, a measure of risk involved in using nonstrategic specifications, such as standards work-in-progress with its inherent risk of change, and those based on non-open specifications. The risk associated with these specifications is based on the premise that the Federal user has virtually no control in the direction that these specifications may take.

The tradeoffs amount to accepting less portability and interoperability in return for meeting current information requirements, and not waiting until all open system specifications become available. This state of affairs is possibly comparable to walking on a frozen river: in some places, it is safe to walk; in others, one must tread carefully. No clearly right or wrong decisions will be made in selecting specifications. Some decisions will be more right than others. Users can only hope with today's technology to ameliorate the effects of long-term changes. NIST will continue to perform evaluations and publish its recommendations. *Users must decide for themselves what is best for them.*

ANNEX A — DOCUMENT SOURCES: CONTACT INFORMATION

The following organizations are responsible for distributing standards for various standards-making organizations. Ordering and fee information for specific standards may be obtained directly from the addressees.

AAP

Association of American Publishers
EPSIG (Electronic Publishing Special Interest Group)
c/o OCLC
6565 Frantz Road
Dublin, OH 43017-0702
Phone: (614) 764-6000

ANSI

American National Standards Institute
1430 Broadway
New York, NY 10018
Phone: (212) 354-3300

ANSI International Publications

Information on standards from ISO and its member bodies (e.g., DIN, BSI, JISC), IEC, and CEN/CENELEC
Phone: (212) 642-4995

ANSI General Sales (National Standards)

Phone: (212) 642-4900

CCITT

International Telegraph and Telephone Consultative Committee
Place des Nations
CH-1211 Geneva 20
Switzerland

COSMIC

Computer Software Management and Information Center
The University of Georgia
382 East Broad Street
Athens, GA 30602
Phone: (706) 542-3265
FAX: (706) 542-4807

Department of Defense

Defense Printing Service Detachment
Standardization Documents Order Desk
700 Robbins Avenue
Philadelphia, PA 19111-5094
Phone: (215) 697-1187
Any Federal organization or DoD contractor can order numerous types of standards, including FIPS PUBs and MIL-STDs from the Defense Printing Service.

Data Interchange Standards Association

ASC X12 and PAEB Secretariat
1800 Diagonal Road, Suite 355
Alexandria, VA 22314
Phone: (703) 548-7005
FAX: (703) 548-5738

ECMA

European Computer Manufacturers Association
Rue du Rhone 114
CH-1204 Geneva
Switzerland
Phone: 011-41-22-735-36-34

Federal Information Processing Standards (FIPS PUB)

U. S. Department of Commerce
National Technical Information Service (NTIS)
Springfield, VA 22161
Phone: (703) 487-4650
FAX: (703) 321-8547
NIST publishes an index of FIPS PUB that is available through NTIS. Request "NIST Publications List 58."

GCA

Graphic Communications Association
199 Daingerfield Road
Alexandria, VA 22314-2888
Phone: (703) 519-8160
FAX: (703) 548-2867

GPO

Government Printing Office
Superintendent of Documents
U. S. Government Printing Office
Washington, DC 20402
Phone: (202) 783-3238

IEC

International Electrotechnical Commission
3 Rue de Varembe
P. O. Box 131
CH-1211 Geneva 20
Switzerland
Phone: 011-41-22-34-01-50

IEEE (for accepted standards)

The Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
P. O. Box 1331
Piscataway, NJ 08855-1331
Phone: (201) 562-3800

IEEE (for draft standards)

1730 Massachusetts Avenue, N. W.
Washington, DC 20036-1903
Phone: (202) 371-0101

ISO

International Organization for Standardization
Central Secretariat
1 Rue de Varembe
P. O. Box 56
CH-1211 Geneva 20
Switzerland
Phone: 011-41-22-34-12-40

JTC1 TAG

Joint Technical Committee 1 Technical Advisory Group
311 First Street NW, Suite 500
Washington, DC 20001
Phone: (202) 737-8888 (Press 1 twice.)

National Computer Graphics Association

2722 Merrike Drive, Suite 200
Fairfax, VA 22031
Phone: (703) 698-9600

National Computer Security Center

INFOSEC Awareness Division
ATTN: IAOC (X711 Ms. Keller)
Ft. George G. Meade, MD 20755-6000

National Technical Information Service (NTIS)

U. S. Department of Commerce
National Technical Information Service (NTIS)
Springfield, VA 22161
Phone: (703) 487-4650
FAX: (703) 321-8547

OSF

Open Software Foundation
11 Cambridge Center
Cambridge, MA 02142

SQL-Access

SQL Access Group
c/o Robert Crutchfield
Fransen and Associates, Inc.
2171 Campus Drive, Suite 260
Irvine, CA 92715
Phone: (714) 752-5942

T1 Standards

Standards Committee T1 Telecommunications
1200 G Street, N.W.
Suite 500
Washington, DC 20005
Phone: (202) 434-8845
FAX: (202) 393-5453

UniForum

2901 Tasman Drive, #201
Santa Clara, CA 95054
Phone: (800) 255-5620 or (408) 986-8840
FAX: (408) 986-1645

UNIX International (UI)

Waterview Corporate Centre
20 Waterview Boulevard
Parsippany, NJ 07054
Phone: (800) 848-6495 or (201) 263-8400
FAX: (201) 263-8401

X3

Technical Committee X3 -- Information Processing Systems
Computer and Business Equipment Manufacturers Association (CBEMA)
Director, X3 Secretariat
311 First Street NW, Suite 500
Washington, DC 20001
Phone: (202) 737-8888 (Press 1 twice.)

X/OPEN — X/OPEN Portability Guide (XPG)

1750 Montgomery Street
San Francisco, CA 94111
Phone: (415) 323-7992

ANNEX B — REFERENCES

"Ada," FIPS PUB 119

"Amendment 1: Realtime Extension [C Language]," IEEE Working Group P1003.4

"Application Software Interface (ASI) Version 1 (for accessing and administering Integrated Services Digital Network [ISDN] services)"

"C," FIPS PUB 160

"COBOL," FIPS PUB 021-3

"Computer Graphics Metafile (CGM)," FIPS PUB 128

"Directory Services Application Program Interface (API)," IEEE Working Group P1224.2

Draft "Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment," IEEE Working Group P1295.1

Draft "Working Implementation Agreements for Open Systems Interconnection Protocols"

"Electronic Data Interchange (EDI)," FIPS PUB 161

"Electronic Manuscript Preparation and Markup (EMPM)," ANSI/NISO Z39.59-1988

"Fortran," FIPS PUB 69-1

"Graphical Kernel System (GKS)," FIPS PUB 120-1

"Government Open System Interconnection Profile (GOSIP) Users' Guide," NIST Special Publication 500-192

"Government Open System Interconnection Profile (GOSIP Version 2.0)," FIPS PUB 146-1

"Information Resource Dictionary System (IRDS)," FIPS PUB 156

"Initial Graphics Exchange Specification (IGES)," FIPS PUB 177

NIST Planned FIPS PUB 127-2 on "Database Language SQL,"

NIST Planned FIPS on "Integrated Services Digital Network (ISDN)"

NIST Planned FIPS PUB on Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities Interface IEEE Std 1003.2-1992, Information Technology—Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities

NIST Planned FIPS PUB on "Standard Page Description Language (SPDL)," ISO/IEC DIS 10180

"Open Document Architecture/Open Document Interchange Format/Open Document Language (ODA/ODIF/ODL)," ISO 8613:1989

"OSF Distributed Computing Environment (DCE) Remote Procedure Call (RPC) Component," Open Software Foundation

"OSI API for File Transfer, Access, and Management (FTAM)," IEEE Working Group P1238.1

"OSI Application Program Interfaces," IEEE Working Group P1238

"Pascal," FIPS PUB 109

"Portable Common Tools Environment (PCTE): Abstract Specification," Standard ECMA-149, European Computer Manufacturers Association (ECMA)

"Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]," FIPS PUB 151-2

"Programmer's Hierarchical Interactive Graphics System (PHIGS)," FIPS PUB 153

"Protocol Independent Interfaces," IEEE Working Group P1003.12

"Reference Model for Frameworks of Software Engineering Environments (Technical Report ECMA TR/55, 2nd Edition)," NIST Special Publication 500-201

"Remote Database Access (RDA)," ISO/IEC 9579:1993

"Security Interface for the Portable Operating System Interface for Computer Environments," IEEE Working Group P1003.6

"Spatial Data Transfer Standard (SDTS)," FIPS PUB 173

"Standard for the Exchange of Product Model Data (STEP)," Draft Proposed ISO 10303

"Standard Generalized Markup Language (SGML)," FIPS PUB 152

"Transparent File Access (TFA)," IEEE Working Group P1003.8

"User Interface Component of Applications Portability Profile," Planned FIPS PUB 158-1

"Version 1.0 Government Network Management Profile (GNMP)," FIPS PUB 179

"X.400 Based Electronic Messaging Application Program Interface (API)," IEEE Working Group P1224.1

ANNEX C — BIBLIOGRAPHY

A Guide for Acquiring Integration Services, Acquisition of Information Resources, U.S. General Services Administration, Information Resources Management Service, Division KMPP, Washington, DC, November 1991, pp. 125.

An Analysis of Application Environments, Emerging Technologies Group, Inc., Dix Hills, NY, 1989, pp. 494.

Draft Model RFP -- Request for Proposals, Federal Computer Acquisition Center (FEDCAC), Boston, MA, as of 17 April 1992, pp. 300+.

Guide to the POSIX Open Systems Environment, Draft 15, IEEE P1003.0, June 1992.

Model RFP -- Request for Proposals, Department of the Air Force, Air Force Computer Acquisition Center (AFCAC), Hanscom Air Force Base, Massachusetts, as of 14 August 1991, pp. 500+. (The major part of AFCAC has been absorbed by the General Services Administration's Federal Computer Acquisition Center [FEDCAC].)

Strategies for Open Systems — Stage Two — The Experience With Open Systems, DMR Group, Inc., Boston, 1990, pp. 196.

INDEX

☆ U.S. GOVERNMENT PRINTING OFFICE: 1993— 341-832/83047

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899